2600

The Hacker Quarterly

Volume Eighteen, Number One!
Spring 2001
$5.00 US, $7.15 CAN

"Why is it perfectly legal to post a diagram of how to build a bomb on the net, but you can't post a code that de-scrambles DVDs?" - The March 3, 2001 edition of "Boon-docks," a daily comic strip written and drawn by Aaron McGruder and seen in newspapers all over the county. It devoted three days to the DeCSS controversy and, unlike virtually all news reports, got the story right.

S T A F F

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate.
Back issues available for 1984-1999 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631-474-2677**

imagine

Signs of Hope

As our appeal of last year's DeCSS case draws closer (at press time it was set to be heard by the Second Circuit Court of Appeals in early May), we realize how much we've accomplished since this whole ordeal started - and how much other people with half a clue have gotten done too. That's not to say that a lot of bad stuff hasn't happened - we know too well about all of that. New bad laws, new threats, more stifling of technology and speech throughout the world. But despite all that, we're going into this with a real feeling of optimism.

As time passes, more people seem to realize the true motives of groups like the Motion Picture Association of America and the Recording Industry Association of America. They're not about protecting the rights of struggling artists, bolstering creativity, or giving consumers a fair deal. They're about maximizing profit - plain and simple. And as things continue to go their way thanks to laws like the Digital Millennium Copyright Act, people slowly start waking up to the reality that maybe their best interests have been completely ignored.

Perhaps the most dramatic display of this overdue realization came in remarks made by Rep. Rick Boucher (D-VA) in early March before a Consumer Electronics Association Conference where he seemed to actually realize the true dangers of the DMCA:

"The time, in my opinion, has come for the Congress to reaffirm the Fair Use Doctrine and to bolster specific fair use rights, which are now at risk. In 1998, responding to the concerns of copyright owners, Congress passed the Digital Millennium Copyright Act. The announced purpose was to protect from piracy copyrighted material in an environment which poses special concerns for copyright owners. They made the point that with digital technology, a copy of a copy of a copy has the same clarity and perfection as the original of the work. They also made the point that in the networked environment, with the single click of a mouse, thousands of those perfect copies can be sent to people throughout the nation and the world.

"The DMCA is the result of the effort by Congress to respond to those realities. There are some today who believe that the legislation went too far. For example, it creates, in Section 1201(a), a new crime of circumventing a technological protection measure that guards access to a copyrighted work. Under Section 1201, the purpose of the circumvention is immaterial. It is a crime to circumvent the password or other gateway, even for the purpose of exercising fair use rights. There is no requirement that the circumvention be for the purpose of infringing the copyrights. Any act of circumvention, without the consent of the copyright owner, is made criminal under Section 1201.

"Some now foresee a time when virtually all new material will be sent to libraries on CD ROMs, with the material encrypted or guarded by passwords. In exchange for a fee for each viewing, the password may then be used. And so it is predicted that under Section 1201, what is available today on the library shelves for free will be available on a pay per use basis only. The student who wants even the most basic access to material to write his term paper will have to pay for each item that he uses.

"Several of us made an effort in 1998 to limit the new crime under Section 1201 to circumvention for the purpose of infringement. But in the momentum to enact the measure, essentially unamended, we were not able to have that change adopted. With the growing realization on the part of the education community and supporters of libraries of the threat to fair use rights which Section 1201 poses, perhaps the time will soon come for a Congressional reexamination of this provision.

"Perhaps the only conduct that should be declared criminal is circumvention for the purpose of infringement. Perhaps a more limited amendment could be crafted to ensure the continued exercise of fair use rights of libraries and in scholastic settings, notwithstanding the provisions of Section 1201.

"And I think there are other challenges. I am concerned by the apparent attempt of some in the content community to seek to protect their copyright interests in material contained in television programs by insisting that the TV signal quality be degraded, or by insisting on the use of set-top box technology which prohibits all copying. The reasonable expectations of television viewers to be able to make copies of programs for time shifting and other historically accepted purposes must be honored and must be fulfilled."

We suspect that there are many others in Congress who feel the same unease but are hesitant to speak out against such powerful lobbies as the MPAA and the RIAA. We must encourage them to listen to the people who elected them, not the special interest groups who use intimidation and money to get what they want.

In another very public display in early March, cartoonist Aaron McGruder devoted his popular comic strip *Boondocks* to the DeCSS controversy. For three days, characters struggled to understand the baffling ruling of Judge Kaplan this past August which forced *2600* to keep the source code off of our site and even banned our linking to other sites that contained this material. "Why is it perfectly legal to post a diagram of how to build a bomb on the net, but you can't post a code that descrambles DVDs?" a character asks a teacher. The rest of the strip is blacked out with the words "CENSORED. We just don't like where he's going with this."

On a different day, the entire strip was replaced with the words: "CENSORED. This comic contains numerous references to the DeCSS code used to bypass the Content Scrambling System of DVDs, which, by order of Judge Lewis Kaplan, is illegal to reproduce in any way. We apologize for the inconvenience, but speech that damages the profits of our corporate friends is NOT protected by the First Amendment. Thank you."

This biting political commentary accomplished in two sentences what virtually every major editorial page has so far failed to do. The sobering consequences of the ruling against us was laid out concisely for all to see. Note that the author *understood* that the code was not designed for copying, a fact that virtually every news report on the subject got wrong.

What this illustrates is that we have allies in places we never even thought of. This one comic strip reached millions of people who now have some understanding of what this case has been, and continues to be, about. There are probably a good many more ways of reaching the public that have yet to be utilized. We need to come up with more ideas and those people who can help get the word out need to come forward.

And of course, technological rebellion continues. We've seen people come up with shorter and more creative methods of bypassing CSS - everything from a DeCSS haiku to a 434 byte C program to a seven line Perl script. There's even a prime number that is identical to the gzip data (in decimal) of the original C source code minus tables. T-shirts, bumper stickers, even tattoos with such "illegal" code are popping up everywhere. And it all serves to illustrate the absurdity of the whole thing.

It's imperative that we keep our sense of humor throughout, no matter how it all turns out. There are many levels on which we could ultimately lose - the court case is only one of them. The spirit of the hacker community is what is vital to this and all future fights. It's an inspiration to many more outside the scene who can only dream of taking on the fights we do. Destiny has put us in this position at this time in history and we have to continue to stand up for those things we believe in - free speech, free communication, free access to knowledge, and the ability to control and shape technology to suit our individual needs.

We're very lucky to be where we are, despite the risks. And we're fortunate beyond words to have such an amazing support network that is still growing and developing. Because no matter how the DeCSS appeal turns out, you can bet there will be more fights in our future. If they open half as many eyes as this case has, they will be worth the trouble.

Police Searches of Computers

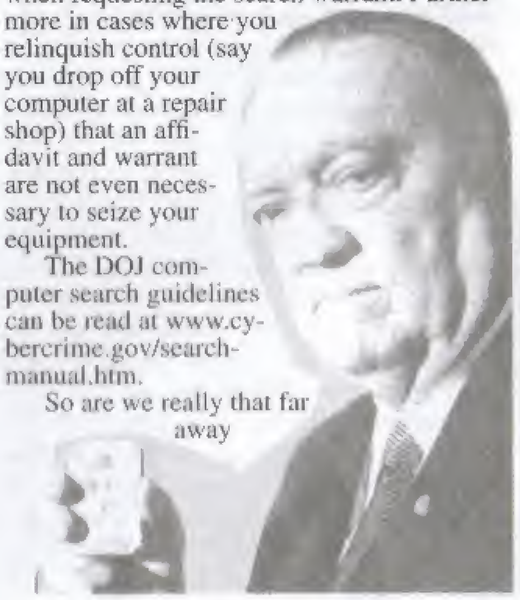
by Todd Garrison

Ignorance of the laws that govern your everyday life is at your own peril. I do not advocate breaking any law, nor do I want to disseminate this article to criminals for the purpose of making the task of law enforcement more difficult. I cannot help but acknowledge that information here can be of use to criminals, but that is mere coincidence because all citizens have the right to protection under the various statutes and rules that protect our freedom.

Because I am involved with information security I have taken it upon myself to become familiarized with state and federal laws that affect computers. I am not a lawyer. I do not offer any of this information as such, nor do I advocate treating any of what I say as authoritative. If you suspect that you may be involved in litigation or an indictment that involves computers, get a lawyer. Not a lawyer who specializes in real-estate law, or general criminal defense. Retain a lawyer who specializes in computer and Internet law. The worst possible situation is a lawyer who doesn't know how the (computer-related) law works and puts you through failed filings while taking the wrong approach to your defense. The prosecutor involved in your case (assuming it is computer-related) will most likely have received specialized training on computer-related offenses. In light of the media circus that surrounds hacking and anything that even remotely relates to a computer crime, prosecutors want to make examples in cases. So expect that they will try for maximum sentence and the harshest punishments for crimes under the guise that future risk can be averted in your case by imposing a harsh sentence before you graduate to more serious crimes.

The inspiration for this article is the recent publication of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," a guide published by the CCIPS (Computer Crime and Intellectual Property Section) of the United States Department of Justice. Anyone who has followed the recent computer crime cases in the press knows that much of the computer crime law is still untested. Every day this becomes less true. Events are rapidly changing the interpretation of laws. Legislation such as the Digital Millennium Copyright Act has shifted fair use away from the individuals our government is supposed to protect and has given the power to large corporations. It will soon be illegal to even reverse engineer a product you have bought, and paid for the right to use - whether for the intended purpose or not. Events such as "sneak and peek" searches are becoming more commonplace when encryption is an issue.

There are, however, steps you can take to protect your privacy and make it more difficult to have certain information and computer systems seized as well as have the ability to recover your equipment after it has been seized. As I said before, I do not advocate or for that matter participate in crimes. It becomes less likely that upon knowing the law that you will be an unknowing party to a crime, but not impossible. For instance you could be implicated in a crime by the fact alone that you know how to use a computer and one of your friends has committed a crime. This situation is not only likely, but happens regularly. Criminal investigators only need a suspicion that you may have information pertaining to evidence in a crime to seize your computers - *even if you did not commit a crime*. There are laws that are supposed to protect against this, sure, but it is just a matter of semantics in the affidavit that the criminal investigator presents to a judge when requesting the search warrant. Furthermore in cases where you relinquish control (say you drop off your computer at a repair shop) that an affidavit and warrant are not even necessary to seize your equipment.



The DOJ computer search guidelines can be read at www.cybercrime.gov/searchmanual.htm.

So are we really that far away from Orwell's *1984*? Does Big Brother have uncontrolled power? No. While you may not be able to prevent the initial show of force - where law enforcement essentially steals your equipment - there are many avenues to protect yourself. When doing vulnerability research on a computer system it is common to investigate multiple avenues of attack. To enumerate as many as possible and explore each one in an intellectual manner before choosing the avenue of attack. This is a discipline gleaned from basic tactics of warfare. It is a tried and proved method of offensive attack and, to be cliche, it is also a great defense. This is what I will attempt to do in this article. I do not propose legal defenses, but merely recognize locations in the existing laws which may allow more room for a defense once you have retained a lawyer.

Warrantless Searches

Quoting Nancy Reagan, "Just say *no!*" ("No, officer, you may not search my vehicle."; "No, officer, you may not enter the premise without a search warrant.") It should be noted here that refusal to search may be deemed as suspicious behavior and under extreme circumstances may be used against you in an affidavit. Keep your wits about you! Your interaction with the police, FBI, prosecutors, etc. will be held against you or will be credited to you during any trials, motions, filings, etc. Generally if they ask to search something they have a reason. Ask why they want to search. If for example they want to search your vehicle for drugs, get it in writing. While this may be something they do not want to do, insist. Make it the *only* condition that they may search. Why? Because if they are looking for drugs as a guise for looking at your laptop, pager, cellphone, PDA, appointment book, etc. they just plain don't have the right. You can't store drugs on your hard disk! Now be extremely careful at this point - if they say they are searching for "evidence" of drugs they may be warranted to look through other devices. Make them change the wording to "drugs or drug paraphernalia" instead of "evidence" before you agree. Note that if they do find drugs, they have the right to search everything, including your computer, etc.

Others may consent to search on your behalf. That's right, even if *you* object, it may not matter. When you were a child you were probably taught that sharing was a good thing. This is true and not true at the same time. Later in this article I will explain when it is good, but in the case of warrantless searches it is not only dangerous, but it is as good as totally relinquishing any control for a search to an officer. The basic idea is your roommate can consent to a search of your apartment. It gets worse. Anyone you share your computer with can consent to its search. Your coworkers can consent to a search, a passenger in your vehicle can consent to a search. Essentially anything that is shared between you and another person can be searched with the consent of the other person. It gets even worse! If for example you don't share your computer with your roommate but they *could* access it, then they can authorize its search too. The search must be limited to what they can access. What this means is that if you must share your computer, do it in a manner that they do not have access to your files. Operating systems intended for a single user should not be considered an option in these cases. Use the multiple users feature of Mac OS 9, use a *nix operating system with different accounts, or use different profiles under Windows NT. Make sure that when you are done using your computer you log out, or employ a screen saver with a password. If you give them your password, then they have the right to give it whoever is conducting the search. Be aware also that operating systems like Windows NT and 2000 may have a common cache for things like your web browser, and since it is accessible by others who use the same computer, then it is fair game and admissible evidence. The best advice I can give is *use encryption* for everything all the time. If you can get away with it, encrypt your applications, their temporary directories, configuration files. The same techniques that you use for protecting yourself against break-ins such as proper registry permissions can help too.

Another reason to employ encryption (and when I say encryption I mean *strong* encryption - always use strong ciphers, not RC2-40bit or DES - but IDEA, 3DES, or Blowfish) is incidental disclosure. If you have a laptop and it gets ripped off on the bus, at the airport, on the subway, at school, or wherever you may be, and they catch the thief - they can search your laptop! They cannot ask for your encryption keys, but anything that the thief could have read (which is everything contained on the laptop), they have the right to read. Now recite this mantra: "Encryption protects me, I will use it everywhere." This type of disclosure opens up a lot of scary questions. Just remember that as long as there are people, there will be people who abuse their power. A criminal investigator may use these circumstance to target you, not that I know of any specific case where this has happened but it is still possible.

Anyone who is involved in security work

knows that passwords, encryption, and physical locks can be overcome. But using these measures, *even if you know they are not completely effective* are an absolute *must*. In the eyes of the law even the weakest encryption affords a level of legal protection regarding allowed access (look at the DMCA). If you took steps to disallow another person from accessing something, no matter how basic those steps are, that means that they did not have legitimate access to those items. If you store your computer in a closed cabinet with a lock and did not give the key to your roommate, they no longer have the right to authorize its access to anyone. Password protect everything, encrypt the most trivial items, use physical locks and keys, store your important removable media in an inexpensive fire-safe. These are all actions that deny access and protect your legal rights against warrantless searches. If you are the only person who has legitimate access to an item, then you are the only one who can release that item for search. But wait! This doesn't apply at work... read on!

There is much debate about expectation of privacy at your workplace. But a basic expectation you should have is - *nothing you do, say, or are otherwise involved in at work is private.* Don't use your e-mail at work for anything private. Don't even send good ol' Mom a message saying hello. Get a free e-mail account that uses SSL or other encryption if you plan on accessing it from work. Better yet, don't even access your private e-mail at work. Your employer has the right to install cameras, listening devices, wiretaps, intercept and archive your e-mail, watch what web sites you visit, and even read your thoughts if they have the technology. The bottom line is keep your private life private. Your employer can, at their discretion, disclose this information to anyone they want. Additionally, they can claim anything you do while on the job as their intellectual property. Don't even risk it. Keep anything you don't want them to know away from their grasp. Expect fully that if you commit a crime that involves computers that your employer will be the first place investigators will search. This is because you essentially have no rights to privacy and very few businesses would resist the will of public authority and deny them a search.

If you travel across borders, leave your laptop at home. Customs agents have the right to an unrestrained search of your belongings, including your data. They can even demand encryption keys, and you have to give them up. Remember that transporting strong encryption outside of the US is considered to be export of munitions, and a federal offense. So even if your data is encrypted, that fact alone could be reason enough to forcibly detain you and even arrest you.

Exigent circumstances: this is when investigators have reason to believe you might destroy evidence. Of all the laws on the books, this is one of the scariest. They don't need a warrant - they don't even have to knock on the door. They require only to have reasonable cause. They don't need evidence or a track record of you doing something like this in the past. They just need a reason to believe it. The intimidating part of this law is that it is up to the investigator, not a judge or district attorney, just the investigator. So if the officer has a hunch that you will try to destroy evidence by deleting files, encrypting data, or disposing of encryption keys once you are alerted to their presence, they have the right to deem a search exigent. Fortunately, because the law is vague, it is seldom used, but it is not unheard of. If you decide to put triggers on your systems that will automagically delete evidence, don't tell anyone about it, not even your friends. Bragging is the most common way people are deemed suspects for a crime and the most likely circumstance that investigators will use to decide you are at risk of destroying evidence.

Warrants

While the above warrantless searches are the most likely that you will be presented with, there is always the chance that a search warrant will be issued. While it can literally be a pain in the ass, it is better to be presented with a warranted search than a warrantless search. If you haven't committed a crime, then you should have reason to believe that the outcome will be in your favor. This is why a warranted search is better. The fact alone that a warrant has been issued means that a judge is involved and can be held accountable for wrongdoings in the legal process. But alas, if there are constraints in warrantless searches, there are even more in searches involving a warrant.

First, the process of how a search warrant is constructed. There are at minimum two documents that must be presented to a judge before he will issue a warrant. The first is an affidavit. This is the sworn testimony of the investigator(s) that show probable cause for a search. It will name what information leads to the conclusion that a search is required, where that information was obtained, and the circumstances under which the investigator believes it relevant. The second is the actual warrant. It describes what is to be searched, what methods will be used, who will be present, where the searched items will be stored, what time frame in which it will be executed, and the overall goal of what is being sought. Search warrants are required to be specific. Once again, searching for evidence of a contraband item is different from searching for an actual contraband item.

No matter what happens, cooperate with the search. Resisting will only make your life difficult. If the warrant specifically states that equipment will be seized, it will have addenda's stating exactly what will be seized, a description of what is to be seized, and what methods will be used to search. The investigators may opt to look through your computer on-site, but this is rather unlikely. If you have the ability, and the warrant does not authorize the seizure of video recording equipment, break out the camcorder and record what they do and say. This may be invaluable evidence in proving that an investigator overstepped the boundaries of a search warrant. It will also prove as a deterrent for them to overstep the warrant at all.

As a citizen you have certain unalienable rights. Use these rights to your advantage. Freedom of speech, attorney-client privilege, privacy of the clergy, freedom of the press, and, as a provider of network services you have more rights than just a citizen by the nature of the rights of those who you provide services to. Let's examine how these issues provide obstacles to law enforcement officials who wish to obtain your shiny new computer.

Freedom of Speech and Freedom of the Press: You have the right to speak your mind and publish those thoughts. These are inalienable rights as a US citizen. Take advantage of these rights. Coincidentally, the Internet happens to be the most available and affordable method to publish your thoughts. Whether it be your business promotions, or social commentary such as this article, *use it!* Update it on a regular basis and make sure it is always available. This is important because if it is never updated or only available when you are surfing the web, the court may dismiss what you have published as not actually being a publication because of it being only occasionally available. Replicate it and make sure that the machines are available as a web server as often as possible - use round-robin DNS to make sure traffic actually goes to *all* of the machines acting as a web server. Any machine that doesn't act as a server for the dissemination of the information should be used to *create* the information being disseminated. Keep your web design software, image editing software, word processor, and proof that they have been used in the creation of your intellectual property that you publish to the Internet on the machines. Are you curious why this is mentioned in an article on search and seizure? Well, you now have the same statutory protections that a newspaper has in regards to search warrants. By seizing tools you use to publish your opinions, they violate many of your rights. Your First Amendment right mostly. These factors will quite possibly cause a search warrant to become more limited in scope and add a likelihood of a time limit upon investigators when removing equipment from your premises. Of course, doing this does absolutely nothing for you if they find you have committed a crime! It will just make them angry, and most likely it will come up in court that you purposely tried to use constitutional privilege to prevent investigators from performing their duties.

Attorney-Client Privilege: Oh boy! This can make an investigator's life difficult. Investigators are required by law to respect documents that contain private attorney-client privileged information. Essentially they can't confiscate them, read them, use them against you, or disclose them to anyone. In case they believe they may inadvertently gain access to such information, they will have to have special exceptions written into the warrant and will have to use an uninterested third party to assist in reviewing the information. If the third party notes that it is privileged information, the investigators cannot use it. Now this brings up interesting consequences. What if the information being sought in the warrant they are executing is actually contained within these documents? I don't know what the outcome would be. I make no claim as to what the result of a legal battle involving steganography hidden information in scanned images of privileged information would be, but I assure you it will be something played out in the courts in the future. In fact, I expect to see it played out in the media too!

Privacy of Clergy and Attorneys: There are special laws involved when law enforcement may search computers or records belonging to lawyers and clergy. If you share your computer systems with people in either of these occupations, investigators will have to get special approval in a search.

Service Providers (or, when sharing your computer is a good thing!): ISPs, phone companies, or anyone providing wire communications to anyone else immediately becomes regulated by the ECPA (Electronic Communications Privacy Act) and the procedures that investigators must use are different. While the folks you provide service to are afforded less privacy by this act (because

searches of a third party system do not require a warrant, only a subpoena), you are afforded more protections and even civil relief in the case of wrongdoing on the part of an investigator.

In short, by executing your rights and providing services to others which allow them to execute their rights you make the likelihood of losing your computers and equipment less likely (assuming that those you provide service for are law abiding as well). Here's a formula for making the seizure of your computer systems less likely. Make a deal with a small local law firm that you will provide them with free web hosting and e-mail services in exchange for consultation of how to gain nonprofit status for your weekly/monthly/whatever Internet-based news publication (e-zine). Scan the documents that you used while conversing with your attorney and use steganography to hide the private keys you use for encryption within those privileged documents. Give away as many free e-mail accounts to your friends and family as possible and encourage them to actively use the accounts. Host a web site and e-mail for a church. Make sure you take the time to show one of the clergy how to use e-mail. Okay, maybe the last suggestion sounds kinda Brady-Bunchish but it may be the motivation for a judge to deny a search warrant.

I'll go ahead and say it again despite recognizing that I sound like a broken record: None of this will help you if you have actually committed a crime. Don't use these methods to make investigators' lives more difficult when you are covering up a crime. It will reflect poorly on you when you receive sentencing. Besides, if you commit crimes you will most likely end up getting caught regardless of what you use your computers to accomplish.

Methods Available to Investigators

If you are being investigated for a crime, there is not a whole lot you can do until you get into a court of law. According to the law, investigators have a wide variety of techniques and are allowed to do quite a bit more than you may expect. Let's look at some of what they can do.

Instrumentality of Crime. If something is used during the committing of a crime, it is an instrument of crime. If you use a computer to break into another computer then the computer you used is an instrument of the crime. But wait - it doesn't stop there. The network you used, the router, the modem, anything that is connected or assists in the function of the system that is the instrument of the crime is considered an instrumentality as well. This can result in blanket seizures of equipment. Generally when searches are conducted against a business, investigators will not seize everything that could be considered an instrumentality. But expect everything computer-related in a search of a private residence to walk out the door. That's just the way it is and the courts support this practice. Once again, our federal government demonstrates that the rights of business are *more important* than those of individuals. Go figure.

No-knock Warrants. Not long ago a man was killed near where I live when the police executed a no-knock warrant at *the wrong address.* The man thought his home was being broken into and armed himself for defense. The police filled him with bullets. Aside from the fact that I believe this to be a blatant violation of the Fourth Amendment, it is dangerous. It puts the lives of law enforcement in danger and it especially puts the lives of innocent citizens at risk. These techniques cost lives, yet judges still approve them. But even scarier yet, in the case that the investigators believe that you may destroy evidence - they don't require a no-knock warrant. They can make the determination and just bust the door in without announcing who they are. The land of the free indeed!

Sneak and Peek. Welcome to the spy age. The government can't spy on the Soviet communist regime anymore, so it has taken to practicing on their own citizens. Bugs, wiretaps, keystroke recorders, cameras, and other covert surveillance techniques previously reserved for national security are now legal and fair game in federal cases. Recently the FBI has used these techniques for capturing keystrokes for getting PGP keys. One such device (pictured) connects to the PS/2 port of a computer and looks fairly innocuous. This model is supposed to represent a ferrite coil which disperses electromagnetic fields. This "bug" only stores about 120,000 keystrokes but there are smaller devices that can store megabytes worth of keystrokes. My suggestion - if you find one of these on your system, take it apart and ensure it *really* is a ferrite coil. If it has anything resembling an integrated circuit inside, put it in the microwave for a few seconds and then throw it away.

Arm yourself with knowledge. Knowing the law helps us all from becoming victims of both crime and the illegitimate practice of law. Defend yourself. Most of all, if you decide to break the law, be prepared for the consequences. Our government no longer is willing to hand out little slaps on the wrist and you can expect to see more extreme measures involved in computer crime.

The Future of PKI

by Elite158

Public Key Infrastructure, or PKI, is a new system (well, new to the public) created by the government to electronically identify yourself. Here I will explain the basic structure of PKI.

The government uses what's called High Assurance Smart Cards, a system known as Fortezza. These smart cards are electronic cards made especially for the government. The cards workers hold contain their personal information. It has, of course, your name, your address, credit card info, SSN, and the whole works. The government uses this system to have authorized workers identify themselves to access classified material. Basically, electronically identifying yourself is an easy and fast way to prove you are who you say you are.

Now Fortezza is coming out to the public, but will be known as PKI or Smart Cards. Even though they're still called Smart Cards, the information will be kept on a more abundant media: the floppy disk. Along with the floppy disk is the laptop PCMCIA card, and possibly even miniCD. These cards, however, aren't High Assurance. Instead it's a Medium/Low Assurance, meaning that the most abundant information is used, instead of putting in every meticulous detail.

PKI will be used mostly in banks and online. In fact, there is a very high chance that by the next election in 2004, people will be able to vote through government servers online, using their Smart Cards. It should work just by sticking in the disk while on their site. The server will gather the information needed, it will do the hand shake if approved, and your vote will be counted.

These cards (remember that these cards are either the floppy disks or laptop cards) are given to you by the government. Now I'm not sure what kind of files the information is stored on, but it has to be some sort of executable program. When you open it up, it'll prompt you for a password. Once typed in and authorized, you have assured yourself that you own that card. You can now use it freely throughout the Internet or wherever the card is applicable. The application will most likely be run in the background. There is, according to the government, no way of tampering with or editing the information on the Smart Card. In fact, to update the information (say you moved or changed your phone number), you would have to take it to a facility like a bank. You would give them what you want to update and they would change it.

These cards are already starting to appear. Visa has got a Smart Credit Card out now. It's a credit card with a microchip on it that contains your personal information, just as I explained. It comes with its own external port that's plugged into your computer. You just stick it in and it acquires the data. This sort of stuff will be seen more often as time passes by.

For right now and not many years ahead, PKI will be voluntary for people to use. But it's likely that in the far future, PKI will become mandatory to everyone 18 and older. It'll basically be a new form of ID, the electronic ID.

This whole system may sound unreal because, just how hard does the government think it would take for a hacker to break the system? There are possibilities now that could make any hacker become well known. The potential of people password cracking their own cards and running around claiming to be someone they're not, or hacking the online voting servers and getting Nader elected, or even making copies with different identities and going wherever they want as whoever they want to be online is remarkable.

In my opinion, this new decade is going to be known as the techno-happy years, where our everyday lives will involve personal usage of technology. Hell, if you think about it, we can already buy our groceries without getting off our asses except to go to the door and pick up the food.

But besides that, PKI is still forming and is still changing. This article was written to give you an idea of what we're in for. Hopefully this new system won't be stupid, but I have high doubts about that. I hope it leaves opportunities for hackers to learn the structure of it, and even manipulation on it. All in all, I hope more people learn about PKI. I will be trying to get more information on it as it progresses.

PHP/CGI VULNERABILITIES AND ABUSES

by L14

PHP is a scripted language primarily used with http servers to create web sites with dynamic, or changing, content. PHP has many similarities to C and Perl, although it is simplified a bit. This makes PHP a nice language with which to work, since many of the complexities that do not concern web site development are removed.

This article will focus on some of the security issues that I encountered while writing a PHP mailing list and helping people on IRC. Most people I talked to did not even realize that security was an issue, and that how their scripts were constructed could change how secure/tamperproof their sites were.

The major problem is how variables are passed to PHP from the web browser. Variables and their values are appended to the URL, resulting in something that looks like this:

http://host/dir/script.php?variable1=somevalue

Because the variable names and their values are passed in plain text from the location bar of the browser, the values can easily be changed by the end user to perform different tasks than what the developer originally intended. Some of the possible abuses of this are described below.

Since many sites are quite complex, and contain scripts that reuse functions, those functions are often put into a standard include file. This means that only one file need be changed to update the entire site. User authentication functions can (and often do) fall into this category. The user is verified once, and thereafter a value is passed to tell further scripts that secure content can be accessed. However in sites with both secure and insecure areas, there needs to be a way of deciding whom to authorize. An easy solution is to just pass a variable that specifies either a secure or insecure mode, depending on what is being linked to. The same things may get executed in both modes but that probably doesn't matter. If the mode is secure and the login fails, the script just bails. If the mode is insecure (or the login is valid), the same core features get executed. The problem of course is that after looking through the site for a few minutes, a user may realize that they could avoid having to login by just changing the value of the mode variable. They can find out what it should be by simply checking a section that does not require authorization, and find out what the mode value is. Then all they have to do is change it in the location bar of the previous page and reload. For a company that has a large audience for its web site or mailing list, this can pose a severe problem: Anyone could change their site with no tools and very little knowledge.

http://host/dir/page.php?var1=val1&var2=val2&mode=sec (user has to login)

http://host/dir/page.php?var1=val1&var2=val2&mode=ins (user doesn't have to login, it's magic!)

This can be solved by moving code related to authentication to a separate file. This file is included instead of the standard include file in documents considered secure, and if the login is valid, the standard file is included as well. This removes the need for a mode variable; removing control is removed from the end-user.

Another problem, identical in its root, is that users can change the values being submitted to make the page work differently. Consider a mailing list: A user visits the page, fills in a form, clicks submit, immediately receives an e-mail with a link in it, clicks the link, and is added to the list. If that user is malicious, they may realize that they can fool with the system by changing the URL in the link, perhaps adding someone else to the list. While this is not much of a problem if they do it once, if they write a simple JavaScript and the mailing list only checks to see if users exist before sending the confirmation e-mail, they can potentially add someone hundreds or thousands of times. If the mailing list only checks to see if users exists before adding them, then the confirmation portion can be abused. The confirmation section, since it sends e-mails immediately, also has more potential as a mail-bombing utility. While trying to abuse my own mailing list software, I managed to send 500 e-mails per minute to my account at university, from a remote computer, using an html/JavaScript file that I wrote at that remote computer and opened in IE. If several sites that were vulnerable in this way were found, quite an effective attack could be launched against major servers, with almost no chance of being caught.

This is also easily fixed. It should be checked both before confirmation and before adding the user whether a given user already exists. There should also be a database of temporary users, which the user subscribing gets added to until they subscribe. This list can be erased periodically, as people may opt to sign up later, but that time should be at least a week. Alternatively, indexes generated from the e-mail addresses themselves could be included in the URL of the confirmation link, so that the address variable and the index variable must match before the user gets added, or a confirmation message sent. This removes the need for a temporary database but can still be tampered with, so in my software I just added the extra database.

I have found this problem in every PHP based mailing list I have looked at, plus several ASP and Perl ones as well. To find vulnerable lists I simply searched for "mail lists" on Yahoo, and if I could manipulate the URL and send my test e-mail account more than one e-mail, I considered it to be vulnerable to attack. To find and test approximately ten, all on reasonably fast servers, took less than 15 minutes, which I feel makes this a legitimate oversight of PHP developers in particular (and CGI developers in general) to look at how program structure can be exploited.

Breaking the Windows Script Encoder

by Mr. Brownstone

The Windows Script Encoder (screnc.exe) is a Microsoft tool that can be used to encode your scripts (i.e., JScript, ASP pages, VBScript). Yes: encode, not encrypt. The use of this tool is to prevent people from looking at or modifying your scripts. Microsoft recommends using the Script Encoder to obfuscate your ASP pages, so in case your server is compromised the hacker would be unable to find out how your ASP applications work.

You can download the Windows Script Encoder at http://msdn.microsoft.com/scripting/default.htm?/scripting/vbscript/download/vbsdown.htm

The documentation already says the following:

"Note that this encoding only prevents casual viewing of your code; it will not prevent the determined hacker from seeing what you've done and how."

Also, an encoded script is protected against tampering and modifications:

"After encoding, if you change even one character in the encoded text, the integrity of the entire script is lost and it can no longer be used."

So we can make the following observations:

* We are a "determined hacker." *grin*

* If it's about "preventing casual viewing," what's wrong with encoding mechanisms like a simple XOR or even uuencode, base64, and URL-encoding?

* Anyone using this tool will be convinced that it's safe to hard-code all usernames, passwords, and "secret" algorithms into their ASP-pages. And any "determined hacker" will be able to get to them anyway.

Okay. So even Microsoft says this can be broken. Can't be difficult then. It wasn't. Writing this article took me at least twice the time I needed for breaking it. But I think this can be a very nice exercise for anyone who wants to learn more about analyzing code like this, with known plaintext, known cypertext, and unknown key and algorithm. (Actually, a COM object that can do the encoding is shipped with IE 5.0, so reverse engineering this will reveal the algorithm, but that's no fun, is it?)

So, How Does This Work?

The Script Encoder works in a very simple way. It takes two parameters: the filename of the file containing the script, and the name of the output file, containing the encoded script.

What part of the file will be encoded depends on the filename extension, as well as on the presence of a so-called "encoding marker." This encoding marker allows you to exclude part of your script from being encoded. This can be very handy for JavaScripts, because the encoded scripts will only work on MSIE 5.0 or higher... (of course this is not an issue for ASP and VB scripts that run on a web server!).

Say you've got this HTML page with a script you want to hide from prying eyes:

```
<HTML>
<HEAD>
<TITLE>Page with secret information</TITLE>
<SCRIPT LANGUAGE="JScript">
<!-//
//**Start Encode**
   alert ("this code should be kept secret!!!!");
//->
</SCRIPT>
</HEAD>
<BODY>
 This page contains secret information.
</BODY>
</HTML>
```

This is what it looks like after running Windows Script Encoder:

```
<HTML>
<HEAD>
<TITLE>Page with secret information</TITLE>
<SCRIPT LANGUAGE="JScript.Encode">
<!-//
//**Start Encode**#@~^QwAAAA==@#@&P~,l^+DDPvEY4kdP1W[n,/tK;V9P4
~V+aY,/nm.nD"Z"eE#p@#@&&JOO@*@#@&qhAAAA==^#~@&
lt;/SCRIPT>
</HEAD>
<BODY>
 This page contains secret information.
</BODY>
</HTML>
```

As you can see, the <script language="..."> has been changed into "JScript.Encode". The Script Encoder uses the Scripting.Encoder COM-object to do the actual encoding. The decoding will be done by the script interpreter itself (so we cannot simply call a Scripting.Decoder, because that doesn't exist).

Okay, Let's Play!

```
Plaintext          Encoded
 Hoi               #@~^FQAAAA==@#@&CGb@#@&zz O@*@#@&WwIAAA==^#~@

 Hai               #@~^FQAAAA==@#@&CCb@#@&zz O@*@#@&TQIAAA==^#~@

 HaiHai
 HaiHai            #@~^IgAAAA==@#@&CCbCmk@#@&CmrCmk@#@&JzRR@*@#@&mgUAAA==^#~@
```

Cute. As you can see, @#@& appears to be a new line (@# = CR, @& = LF), and the position of a character does (sometimes...) matter (the first time HaiHai becomes CCbCmk and the second time it's CmrCmk). Let's just encode a line with a lot of A's:

```
//**Start
Encode**#@~^lgAAAA==@#@&b)zbzbbzbz)bzb)bzb))zbbz)bzbbz))bzbzb)b))zb)bz)bzb))zbb))zb)bz
))zb)zbzbbzbz)bzb)bzb))zbbz)bzbbz))bzbzb)b))zb)bz)bzb))zbb))zb)bz)zb)zb@#@&zJO @*@#@&vyI
    AAA==^#~@
```

The Algorithm

After staring at this for some time, I discovered that the bold part was repeating (actually, the entire string is repeating itself after 64 characters). Also, it seems to be that the character "A" has three different representations: b, z, and). If you encode a string of B's you'll see the same pattern, but with different characters.

This means the encoding will look something like this:

```
int pick_encoding[64] = {...};
int lookuptable[96][3] = {...};

char encode_char (char c, int pos)
{
   if (!specialchar (c))
      return lookuptable [c-32][pick_encoding[pos%64]];
   else
      return escapedchar (c);
}
```

I assumed that only the ASCII codes 32 to 126 inclusive, and 9 (TAB) are encoded. The rest are being escaped in a similar fashion as CR and LF.

What's left is the stuff before and after the encoded string. I did not look into this (yet). It will probably contain a checksum and some information about the length of the encoded script.

The Encoding Tables

So now we'll have to find out those tables for the encoding. The pick_encoding table is very simple to discover by just looking at the pattern that was the result of encoding all those A's.

```
int pick_encoding[64] =
{
   1, 2, 0, 1, 2, 0, 2, 0, 0, 2, 0, 2, 1, 0, 2, 0,
   1, 0, 2, 0, 1, 1, 2, 0, 0, 2, 1, 0, 2, 0, 0, 2,
   1, 1, 0, 2, 0, 2, 0, 1, 0, 1, 1, 2, 0, 1, 0, 2,
   1, 0, 2, 0, 1, 1, 2, 0, 0, 1, 1, 2, 0, 1, 0, 2
};
```

The string of A's had a CR and LF in front of them, so after skipping the first two digits, you'll see that 0, 1, 2, 0, 2, 0, 0, 2 perfectly matches b,), z, b, z, b, b, z , having b=0,)=1 and z=2.

The other table is a matrix that holds three different representations for each character. Which one will be used depends on the pick_encoding table. To find out this matrix, just make a file that will cause every character to be encoded three times. Make sure the algorithm is "reset" by padding the lines so each group will start on a 64-byte boundary.

```
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
!!!aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
"""aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
###aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$$$aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Etcetera. Note that there are only 59 bytes of padding a's because the CR and LF at the end of the line are counting too! (59 + 2 + 3 = 64).

After encoding this you can remove the encoded a's again, as well as the @#@& for the CR and LF. This is what remains:

```
d7i P~, "Ze JEr a:{ ^yf ]Yu ['L BvE `cv #b* eMC _Q3 ~SB OR  R c z&J !TZ Fq8  +y &f2 c*W
*X1
v+ G{P %0R ,1O )l= iIp @!@!@! 'x{ @*@*@* q_Q @$@$@$ b)z A$~ Z/; f9G 23A sow M!V Cu_ q(&
9Bx |Fn      SJd H\t lHg r6} nKh p}5 I]" ?j
U KP: ji` ;#j   q (po 5eI }t\ $,] -w' TDY 77% {m| =|# lCm 48( m^l N(9 +n 0W6 oLT t44 krb
L%N 3V0 Vs^ :hs xU      WGK w2a ;5$ D
.M /dk YOD E;! \-7 hAS 6aX XzH y".      `P uk- 8N) U=?
```

So what is this? It's the encoded representation of the ASCII characters 9, and 32 through 126. Every character has got three different representations, so this sums up to 3*(127-32 + 1) = 288 characters.

You'll see that the < , >, and @ characters are escaped too, resulting in the following table:

```
Esc     Org
 @#      \r
 @&      \n
 @!      <
 @*       >
 @$      @
```

I've removed the @!, @* and @$ from the encoded text too and replaced them with question marks, so the table will stay nice. This is what you get as a hex dump:

```
unsigned char encoding[288] = {
        0x64,0x37,0x69,  0x50,0x7E,0x2C,  0x22,0x5A,0x65,  0x4A,0x45,0x72,
        0x61,0x3A,0x5B,  0x5E,0x79,0x66,  0x5D,0x59,0x75,  0x5B,0x27,0x4C,
        0x42,0x76,0x45,  0x60,0x63,0x76,  0x23,0x62,0x2A,  0x65,0x4D,0x43,
        0x5F,0x51,0x33,  0x7E,0x53,0x42,  0x4F,0x52,0x20,  0x52,0x20,0x63,
        0x7A,0x26,0x4A,  0x21,0x54,0x5A,  0x46,0x71,0x38,  0x20,0x2B,0x79,
        0x26,0x66,0x32,  0x63,0x2A,0x57,  0x2A,0x58,0x6C,  0x76,0x7F,0x2B,
        0x47,0x7B,0x46,  0x25,0x30,0x52,  0x2C,0x31,0x4F,  0x29,0x6C,0x3D,
        0x69,0x49,0x70,  0x3F,0x3F,0x3F,  0x27,0x78,0x7B,  0x3F,0x3F,0x3F,
        0x67,0x5F,0x51,  0x3F,0x3F,0x3F,  0x62,0x29,0x7A,  0x41,0x24,0x7E,
        0x5A,0x2F,0x3B,  0x66,0x39,0x47,  0x32,0x33,0x41,  0x73,0x6F,0x77,
        0x4D,0x21,0x56,  0x43,0x75,0x5F,  0x71,0x28,0x26,  0x39,0x42,0x78,
        0x7C,0x46,0x6E,  0x53,0x4A,0x64,  0x48,0x5C,0x74,  0x31,0x48,0x67,
        0x72,0x36,0x7D,  0x6E,0x4B,0x68,  0x70,0x7D,0x35,  0x49,0x5D,0x22,
        0x3F,0x6A,0x55,  0x4B,0x50,0x3A,  0x6A,0x69,0x60,  0x2E,0x23,0x6A,
        0x7F,0x09,0x71,  0x28,0x70,0x6F,  0x35,0x65,0x49,  0x7D,0x74,0x5C,
        0x24,0x2C,0x5D,  0x2D,0x77,0x27,  0x54,0x44,0x59,  0x37,0x3F,0x25,
        0x7B,0x6D,0x7C,  0x3D,0x7C,0x23,  0x6C,0x43,0x6D,  0x34,0x38,0x28,
        0x6D,0x5E,0x31,  0x4E,0x5B,0x39,  0x2B,0x6E,0x7F,  0x30,0x57,0x36,
        0x6F,0x4C,0x54,  0x74,0x34,0x34,  0x6B,0x72,0x62,  0x4C,0x25,0x4E,
        0x33,0x56,0x30,  0x56,0x73,0x5E,  0x3A,0x68,0x73,  0x78,0x55,0x09,
        0x57,0x47,0x4B,  0x77,0x32,0x61,  0x3B,0x35,0x24,  0x44,0x2E,0x4D,
        0x2F,0x64,0x6B,  0x59,0x4F,0x44,  0x45,0x3B,0x21,  0x5C,0x2D,0x37,
        0x68,0x41,0x53,  0x36,0x61,0x58,  0x58,0x7A,0x48,  0x79,0x22,0x2E,
        0x09,0x60,0x50,  0x75,0x6B,0x2D,  0x38,0x4E,0x29,  0x55,0x3D,0x3F
} ;
```

So, encoding character c at position i goes as follows:

* look up which representation to use (the first, second or third): pick_encoding[i mod 64]
* find the representations in the huge table: encoding[c * 3]
* encoded character = encoding[c*3 + pick_encoding[i%64]];

Because the table starts at 9 and then goes to 32, you'll have to do some corrections. But we'll get to that later, as we are not really interested in encoding after all. We want to be able to do some decoding!

The Decoding Tables

The pick_encoding table will stay the same. This is because each character (except for the escaped ones, of course) will be in the same place as the original. Then, we could just look up the encoded character in the table. For instance, an "A" in encoded text (hex 0x41), occurs on these places in the "encoding" table:

* row 9, group 4, representation 1 = "F"
* row 10, group 3, representation 3 = "I"
* row 23, group 1, representation 2 = "{"

So an "A" in the encoded text is an F, I, or {, depending on its position. Where there is a 0 in the pick_encoding table, it's an F, for 1 it's an I, and for 2 it's a {.

You don't want to go looking through the encoding table each time trying to find those numbers. By transforming the encoding table into another table, you can just go to position 0x41 (actually, 0x41 - 31 to correct it skipping everything below space except for TAB), and pick the correct representation.

```
unsigned char transformed[3][126];

void maketrans (void)
{
        int i, j;

        for (i=31; i<=126; i++)
             for (j=0; j<3; j++)
                  transformed[j][encoding[(i-31)*3 + j]] = (i==31) ? 9 : i;
}
```

With this matrix, it's very simple to look up the original character by simply looking it up in our table. Assume i is the position of the character and c is the character again. Then:


```
decoded = transformed[pick_encoding[i%64]][c];
```

The Encoding of the Length-field

So what's left is to find out how many characters there are to decode. If we just keep decoding stuff, we will decode part of the HTML that's behind the encoded script. This can be avoided by stopping when a "<" is encountered ("<" will never appear in an encoded stream), but even in the case where we are looking at a "pure" script file (*.js or *.vbs), there is some checksum stuff behind the actual data, which we should not decode.

I created a number of files of different size. By giving them a *.js extension the entire file is encoded without the Script Encoder looking for a start marker. The results are below (only the first 12 bytes are displayed).

Length	First 12 bytes	ASCII
1	23 40 7E 5E 41 51 41 41-41 41 3D 3D	#@^EQAAAA==
2	23 40 7E 5E 41 67 41 41-41 41 3D 3D	#@^EgAAAA==
3	23 40 7E 5E 41 77 41 41-41 41 3D 3D	#@^EwAAAA==
4	23 40 7E 5E 42 41 41 41-41 41 3D 3D	#@^FAAAAA==
5	23 40 7E 5E 42 51 41 41-41 41 3D 3D	#@^FQAAAA==
6	23 40 7E 5E 42 67 41 41-41 41 3D 3D	#@^FgAAAA==
7	23 40 7E 5E 42 77 41 41-41 41 3D 3D	#@^FwAAAA==
8	23 40 7E 5E 43 41 41 41-41 41 3D 3D	#@^GAAAAA==
9	23 40 7E 5E 43 51 41 41-41 41 3D 3D	#@^GQAAAA==
32	23 40 7E 5E 49 41 41 41-41 41 3D 3D	#@^IAAAAA==
48	23 40 7E 5E 4D 41 41 41-41 41 3D 3D	#@^MAAAAA==
80	23 40 7E 5E 55 41 41 41-41 41 3D 3D	#@^UAAAAA==
96	23 40 7E 5E 59 41 41 41-41 41 3D 3D	#@^YAAAAA==
103	23 40 7E 5E 5A 77 41 41-41 41 3D 3D	#@^ZwAAAA==
104	23 40 7E 5E 61 41 41 41-41 41 3D 3D	#@^aAAAAA==
111	23 40 7E 5E 62 77 41 41-41 41 3D 3D	#@^bwAAAA==
116	23 40 7E 5E 64 41 41 41-41 41 3D 3D	#@^dAAAAA==
166	23 40 7E 5E 70 67 41 41-41 41 3D 3D	#@^pgAAAA==
216	23 40 7E 5E 32 41 41 41-41 41 3D 3D	#@^2AAAAA==
265	23 40 7E 5E 43 51 45 41-41 41 3D 3D	#@^CQEAAA==
451	23 40 7E 5E 77 77 45 41-41 41 3D 3D	#@^wwEAAA==

The length seems to be encoded in the 5th to 10th byte, and 41 appears to be representing zero. The first byte of the length seems to be increasing with one when the length increases with four. Also, the second byte alternates between 41, 51, 67, and 77.

If you look at length 166, this value is 0x70, where it should be 0x41 + (166/4) = 0x6a. So something goes wrong, and it can be narrowed down to length 104, where it suddenly jumps from 0x5a to 0x61. This puzzled me for a long time, until I realized that 0x5a = "Z" and 0x61 = "a". And yes, the length turns out to be Base64 encoded indeed!

The Checksum

At the end of the encoded data is apparently some kind of checksum. I did not look into this any further.

The Decoder Program

The further working of the decoder program, which can be downloaded from the scrdec home page, is left as an exercise to the reader. It's implemented as a "Turing-like" state machine. The decoder will treat .js and .vbs files as fully encoded, while .htm(l) and .asp files are seen as files that contain script amongst other things - like HTML code.

The decoder simply takes two arguments: input filename (encoded), and output filename (decoded).

There is one thing lacking in the decoder: the value of the <SCRIPT LANGUAGE="..."> attribute is not changed back into the original form. You'd better use a tool like sed for that.

Conclusion

It's not just sad that Microsoft made a tool like this. They've probably asked Bill Gates' little nephew to write this code. The really bad part is that Microsoft actually recommends that people use this piece of crap and, because of that, people will rely on it, even though the documentation hints that it's unsafe. (Nobody reads the docs anyway....)

Security by obscurity is a bad, bad idea. Instead of encouraging that approach, Microsoft should encourage programmers to find other ways to store their passwords and sensitive data, and tell them that an algorithm or any other piece of code that needs to be "hidden" is just bad design.

This article originally appeared in the Dutch hacker zine 't Klaphek. They can be found at www.klaphek.nl. See this issue's Marketplace for info on their monthly meetings.

LIBERATING ADVANTS TERMINALS

by Loki

You may have seen these floating around in your hometown. They are relatively new Internet kiosks called "Advants Terminals" (www.advants.com). With a price like $1 for five minutes it's almost a crime to even use these things. So the following is my ordeal with liberating one of these terminals that resides in a coffee shop in my hometown.

One day I walked into my local hangout to get a coffee and when I went to sit down with my beverage I noticed a computer looking thing on a low table in the corner. Almost immediately I went into hack mode. Many a question ran through my head such as: what OS is it running, what kind of connection does it have, what are the systems specs, can I run quake and most importantly how can I use it for free. Well here's the low down people.

All of the Advants terminals I've come across have been Wintel boxes: * gig HD, 500mhz Celeron, 48 megs of ram, and an ATI Rage 128 video card. To keep the kiosk "secure" instead of running the normal Windows Explorer shell, it runs a program called "Netshift" (www.netshift.com). As long as it is running this, pretty much all useful operations are impossible. So to get started the first thing I did was pull the plug. When I tried this I found that the plug was somehow attached to the wall. They did this by having a screw go into the ground plug at a diagonal and putting pressure on the inside of the ground plug hole. To get past this all you have to do is reach under and unscrew until the plug comes out of the wall. Now, since the beginning of my experiments with this kiosk they have upped the security a bit by encasing most of the computer in a larger cabinet (sort of like a standup arcade game) and putting in a relatively useless UPS (Uninterruptible Power Supply). If the machine doesn't turn off when you pull the plug you should hear a beeping in the lower part of the cabinet. If you are using one of the smaller "desktop" terminals it should just go off immediately.

When you plug the box back in it will power up. Now this is where it may be different from box to box. The screen may or may not be scrambled while this happens. The box I play with started out not being scrambled, then was, and now isn't. So you may have to do the rest of this without being able to clearly see the screen (don't worry, it isn't that hard). You will get your normal boot thingy (yes, that's a technical term). CMOS is *always* passworded in my experience but if you want to screw with it, that's your prerogative. To get to it just hit delete as usual. I won't go into that because I haven't messed with it (yet).

Just after it is finished with the RAM and HD check is your chance to get into DOS, hit Ctrl-Esc (not F8), and you should get the Windows "safe mode" boot prompt letting you choose Safe-mode, Normal Boot, or DOS and a few other little options. Now this takes a little timing and finesse but it can be done, so don't be discouraged it you see a Windows 95 loading splash screen - just hit Ctrl-Alt-Del and go at it again. Once you get to this stage you're just about half done. For you people with a scrambled screen, you should see a somewhat recognizable white bar across your scrambled screen that means you've got it.

Now hit 6 and enter. This will get you the DOS prompt. For you people with scrambled screens, type "cls" and enter to see if it clears the screen. If so, you've got it. From here it defaults to C:/ so you're going to have to go to the Windows directory (cd Windows). Now here is the tricky part for you people who are doing this blind. Type "edit system.ini" and you should get a blue screen that is the familiar DOS edit program. Now we are going to change the shell from Netshift to Explorer. Now hit the down arrow two times and enter a "//". This will comment out the "shell=netshift/naska.exe" line. Then hold down the "fn" key and that will turn the right arrow key into the end key, so basically "shift-end" will move your cursor to the end of the line. Now hit enter and type "shell=explorer.exe". Don't mess up because this could cost you the box if you botch it. It should look something like this:

[boot]
oemfonts.fon=vgaoem.fon
//shell=netshift/naska.exe
shell=explorer.exe
system.drv=system.drv
drivers=mmsystem.dll power.drv

"Alt-F" followed by "X" and "enter" will save and exit you back to the DOS prompt. Now type "Win" and hit "enter" and you're on your way to a free net box. The power supply is ATX and if it boots into Windows and you typed the shell wrong it'll try to shut down. Shutting down means you either have to get inside the locked case to turn it back on or you have to call Advants and wait for them to come back out and fix it (I've had to do this three times!). If it says something about it being a bad shell or something, *pull the plug* and go again.

Now if that sounds like a real bummer to do blind, you're in luck. There is another way, but I felt like explaining the way I did it my first time. The way I just explained is the most fun and the most hackish. It's also the quickest and has the least potential for destruction of the box, especially if the screen isn't scrambled. The box, when it is running Netshift runs War_FTP and most of the boxes allow anonymous access. There are two ways you can take advantage of this. They both involve getting the box's IP. To do this click the free C-NET button, and use C-NET's web search. Search for "your IP". This will locate a site that will show you your IP when you visit it. Now that you have that, you can do one of two things. One, you can go home, ftp to the box, download the system.ini, edit it and re-upload it, then go back to the box and reboot. Or you can get something called VNC (www.uk.research.att.com/vnc/). With this prog you can log into your own box from the net and see your desktop in real time. So once you have VNC on your box at home, all you have to do is put a dollar into the Advant's box, type your home IP into the "goto" form and you'll get your home desktop. From there you can use that even after your time runs out to do whatever you want on your home box because the page address never changes so it won't kick you off. This is helpful because you can now upload things from your home box to the Advant's box, such as a new system.ini.

If everything worked out right you should be in Windows and you can have all the fun you want exploring around. Just remember - when you're done put it back to NetShift so some "K-Rad Elyte H4x0r" doesn't come along and destroy the box or shut it down. You can then have fun later the next time you want to use the box. Don't forget to share your free net access while you're supervising. People will appreciate it more than you know and you're bound to make a few friends that way.

I personally have put GLQuake on the box that I use and it runs pretty well. The connection is most likely a crappy DSL shared on a LAN modem somewhere so it's not really suited for much. I've seen it get 15k a sec but it usually gets 5-7. The IP range from what I've seen is 38.28.129.* and 38.28.130.* if you'd like to scan for the boxes. I've yet to have any luck that way though.

It says on Advant's web site that they will soon be switching to the Linux OS to bring down the cost of the box and thus lower Internet prices. When they do that, I'll get on top of it and write a follow-up article on liberating the new OS.

I'd also like to give props to my man Agile for being there for moral support, free drinks, and more than one time preventing me from doing stupid crap (and hitting me when I did do something stupid).

A Romp Through System Security

by Lumikant with help from Zarium

So you have your web server, you've got millions of hits on your web site every day, but you feel that ever-present nagging feeling inside that there's something missing. You're right, something is always missing - it's called security. "So, how do I secure this beast of mine here?" you may ask. In this article, you'll see some ways of going about it. However, this is in no way a complete guide to security, but rather a cornerstone, or a foundation, in learning the basics on UNIX and UNIX variant security. Topics covered will include basic software security, hardware security, and general common sense techniques to prevent your system from getting owned. Well, that's enough yackin, let's get to hackin!

It's assumed you have general knowledge of a *nix based system. All the methods herein have been tested on a Slackware 7.1 system, as well as a Red Hat 6.2 system. These are two common distributions of Linux that are often used for web servers. We're also assuming that the computer the server is on is an up to date computer (at least 300 mhz, 128 megs of ram) that can easily be used for a web server. Hopefully you are running *at least* kernel 2.2.16, or a development version written around that kernel. Some of the methods in this article will be of no avail or may not work if the kernel is a lower version than that. A side note here - always get the latest stable kernel running on your system. With every new release comes new bug fixes, new updates, and support. Security isn't a one-time fix-all, but rather a careful ever-watching vigilance over your system/network.

This article is also written specifically for securing a web server that hosts a web site. If you intend to use the system for more than just that, be careful how you follow what is described in this text, because the methods may cripple other vital services that you'd need in other situations. It does however allow for optional POP3 e-mail usage through a local SMTP server. However, unless you need it, we recommend you drop that service. Being as just about anything is exploitable, it's only a matter of time until someone uses that service against you. (Yes, paranoia is a *good* thing here, guys.)

Finally, we are assuming you have local access to the server itself. If you can only admin the box remotely you will have to allow certain exploitable services that I would suggest disallowing and/or killing. Services such as ftpd and telnetd. After all, if you can dig into it remotely, that means somebody else most certainly can.

The basics of securing a web server are often the most neglected. Admins seem to be sloppy when it comes to this, the most important part of securing a server. What good are all the patches in the world, all the firewalls and other various software, if your kernel is exploitable or if other users have a great deal of access? Not very is the correct answer (give yourself a pat on the back if you got that one, but not too hard, you may pull a muscle).

The Kernel

The kernel is the core of a *nix system. In fact, it is almost the entire system itself. The kernel is notated for its version. For example, the latest stable kernel at the time of this writing is 2.2.18. The version of a kernel has two parts, the kernel version (first and second fields) and the patch level (third field). Kernel 2.2.18, for example, means that 2.2 is the kernel version and 18 is the patch level of this specific kernel. If the kernel version itself is an odd number (i.e., 2.3), then it's a development kernel. This is not a stable release and should not be used unless you're a programmer or Unix Guru. In that case, use it by all means, improve it, re-code it, work on it, and then tell everyone out there so they can help improve it too. Development versions oftentimes have many bugs that are easily exploitable. Unless you are a Unix Guru, you should not run a development version of a kernel. The latest kernel can normally be found at in the Freshmeat archives (for Linux): www.freshmeat.net/.

Root Account

Another security issue admins often overlook is the usage of the root account. For most work you do, the root account isn't needed. This is an important point to make. When you mess with the root account, you are playing with fire. You don't get pretty little error messages with UNIX like you do with Windows if you say "Delete this." It does it - no recycle bin. It's an unnecessary risk, especially if you are running an xterm. Not only can you make mistakes as root that can compromise system security, it also makes it more difficult to see when others have been accessing the root account, which is an important step in finding out who owned you.

The easiest way to avoid problems with root is to make another user account - using the "adduser" command - and give that account admin permissions. This will allow most actions, but will keep you from causing wanton damage to the system and make it easier to notice unwanted activity as root. It also makes for a safer xterm environment, disallowing someone from crashing your entire system remotely through an xterm buffer overflow.

Shell Accounts

Sometimes other people, friends, associates, and otherwise will want an account on your system, be it for their own web page, use of the services, etc. This is okay! It's one of the beauties of running a *nix system - allowing multiple users to log in. However, just like the Force, this has a dark side. If one of your friend's accounts is cracked, that person loses whatever privacy they had with their files and gives the intruder a launching place to root you. Give shell accounts out to only the most trusted of people. Another great aspect of Linux is the ability to use different group ID's. Put all users into a group such as games so they have little to no access to exploitable system services. A practice that is becoming more and more popular nowadays is to simply block out port 23, the telnet login port, disallowing shell accounts. While this is a clever way of keeping you from being rooted, it also crimps the beauty and ability of *nix systems.

Services

Now let's move on to many of the services and daemons that keep a *nix system running well. If the kernel is the base, the skeleton, of a *nix system, then the services and daemons are the blood, muscles, and skin. They are what complete tasks, allow external users, post your web page, etc. They're also what allow the easiest entry into your system, so do be careful. Several services are very important to you if you're running a web server. The most important of these is the Hyper-Text Transfer Protocol Daemon, or httpd. This is the daemon that actually opens port 80 for HTTP traffic, thus allowing your site to be viewed. This service is *not* standard on a *nix system. It comes with whatever web server you choose. This daemon in and of itself is very secure.

Another daemon that is almost as necessary as the httpd is the crond. This daemon watches all the programs on your cron tab (a list of programs that should always be running), and if one of them is down, inactive, absent, or frozen, it begins the program anew to make sure the program is running. If the initialization program for the web server is on the cron tab, whenever it crashes it will be started again, thus keeping the page up.

Many services and daemons however are unnecessary and are very insecure. These services should be killed and whenever possible disallowed from starting in the first place These services are what allow most defacements and intrusions.

fingerd

The most unnecessary and dangerous service is the fingerd. The finger daemon, running on port 79, is also useless. The sole purpose of it is to give out information about your users. As if that's not dangerous enough, it is also a very easy service to crash, most often through a buffer overflow, to give one a root access shell. Here is a finger response from a WindowsNT webserver running worldgroup.

Crystal Mountain BBS
User-ID: Sysop
E-mail alias: Sysop@wgserv.crystal-mtn.com
Sorry, that User-ID has not filled out a Registry entry...

This is an example of finger information from a *nix based system.

Login: root Name: Root - Bilbo or Garfield
Directory: /bywater/admins/root Shell: /usr/local/bin/bash
Last login Sat Nov 25 16:33 (CST) on ttyC0
Mail last read Wed Dec 13 05:04 2000 (CST)
No Plan.

As may be apparent to you, this offers quite a bit of information that could be used by someone wishing to infiltrate a system. It gives the shell type used (bash), home directory, real name (in some cases), last login, and last time the mail was read. Sometimes the plan can show even more important information. All of that coupled with the buffer overflow possibility makes this service very dangerous. It should be removed from your initialization files (usually /etc/inetd.conf - just comment out the lines that start this service. Other places you could look are the /etc/rc.d/ where several files may exist that manage your startup services. This is going to be different with every flavor of Unix out there.)

ftpd

Another service that is easily exploitable is the ftpd (File Transfer Protocol Daemon). This daemon allows people to access files on your system, as well as send files of their own. The danger in this is pretty self explanatory. Although this protocol is often used and is reasonably secure, it is still a risk.

Depending on the version of ftpd you run, it may be possible to download password files and other sensitive materials through FTP, so make

sure that you have your users set and restricted enough to where they're not even allowed read access to the /etc directory in particular, or if you're paranoid enough, any directory other than their own and anything in the FTP directory.

One version of ftpd, WUftp, is the absolute worst ftpd one can run. It has so many exploitable bugs, it makes for a playground for any intruder who wishes to cause your server harm. People have been known to scan entire IP blocks (i.e., 209.23.*.*) for servers running this daemon, just for a little easy fun. Pretty sick, isn't it?

If you have other users or wish to update your server or web page remotely you will need the ftpd. Just make sure you have the newest version with any necessary patches. This will save you from a lot of trouble in the long run. If you're not going to be updating remotely then kill the ftpd. It's recommended you do all your updates right there on the server if possible.

telnetd

Another service that you won't need unless you plan on having extra users is the telnetd. This daemon, which runs on port 23, allows users to access a remote console of your system. This, while being a secure service itself, allows for many problems.

Basically, the only way to break in through the telnetd is with a simple brute force attack. This throws as many passwords as it can to your computer, hoping one is right. If you have a strong password this attack is almost useless but there's still a chance that someone could gain access. If you are only offering web space to the people who have accounts on your system, then giving them access to telnet is also unnecessary because this allows them to try all sorts of local exploits on your system. Local exploits often are more effective due to the easier access to the system. All in all, telnetd is unnecessary to be running unless you have users who want to use the shell services of your server. If you don't have any of those users, the smartest thing to do would be kill the telnetd.

smtpd

Another service that is nice to have if you are offering e-mail services is the smtpd. This is the service that allows your server to send and receive mail. This service is secure in the way that it doesn't allow ready access to your system. However it's insecure in the way that it's easy to monitor traffic in and out of it. It also allows people to send e-mail without their true identity showing up.

These problems can be remedied by simply using the newest and patched version of SMTP, or ESMTP (Enhanced Simple Mail Transfer Protocol). Also, make sure any important e-mail you send is encrypted, preferably with PGP, so snoopers won't get any sensitive information.

Keep Watching Your System!

Another very important part of keeping your system secure is keeping up with all the current bugs and exploits and, more importantly, their patches and fixes. Something as simple as an outdated and buggy service can allow someone access to your system. Not only do these bugs, or exploits as they are most often called, sometimes provide access to your system, they can also allow malicious users to view sensitive data or crash your system. This, for the most part, can be easily avoided with simple measures such as always using the newest release of a service or piece of software. Take Perl for example. This service allows you and other users to make web based (and other) scripts, including CGI, which can allow someone to gain root on your system if they have a shell. However in the newest versions of Perl, the SUID exploit, as it is called, has been patched.

Perl

Perl scripts, if not written carefully, can also allow users to view data. Because they run on a shell and interact with your system, they can often be "tricked" into displaying information. Also, if the files it refers to don't have stringent permissions, then someone could view files dealing directly with the script.

Logs

No, we're not talking about those things that you burn in the stove. Logs are *very*, mucho, uber important to your system. With these handy things, you can see who broke in, from what IP address they were hailing, and at what time (among other things). You've got to log *every* connection, and for you paranoid people out there, *every* single *packet* that comes into your system. A firewall can accomplish this rather easily, but your system will also log failed telnet logins. If you notice that a certain IP attempted to login as a user several times and failed, then you might consider restricting that account and banning that IP address, being as someone is very likely to be trying to brute force their password. Your system also logs odd happenings. Pay attention to your logs. If you get owned, you'd better be able to prove how when you go whining to the authorities. System logs are usually appended in a file located in /var/log/messages.

Passwords

One thing your users need to have is a strong password. This basically means that if their password is their first name (i.e., jerry), then you've got a problem. Let's say Jerry has a friend at school who wants to thrash a Unix box somewhere. He knows Jerry's username on bleh.org is "dude". So he goes in and brute forces the password. Since he knows Jerry, he's going to guess things that are close, near, and dear to him, such as his girlfriend's name, his dog's name, his mother's name, his car, his favorite movie, etc. Finally, the intruder enters "jerry" as the password and he's allowed in. From there he downloads local exploits and roots your sorry rear. Tsk tsk, if you would have been a good little sysadmin, this could have been avoided. You should have Jerry change his password every three months (i.e., every business quarter or whenever you feel it would be a good time, as long as it's somewhat often). Make sure Jerry's password isn't something like "laura" (maybe his wife's name?). That's just dumb, because *anyone* who knows Jerry and is trying to guess his password is going to know Laura more than likely and try guessing that as his password. Make him use something off the wall and totally random, like 77x883492xxsofyBB25.8. The longer the password, the better, as it takes a dictionary creator and/or password cracker much longer to reach a password of this length than it does "laura". Also, even though it may be hard to remember, it's still feasible to create a password within a password. For example, let's say your dog's name was "Missy" (like my mom's little dachshund, God rest her soul). Let's say you have a work ID number of 12345. Try this: 1m2i3s4s5y. This spells "missy" with 12345 strewn through it. Although this method is commonly used, it is a bit more difficult to crack.

Firewalls

Firewalls are super-handy. Make sure you're running one on the gateway in your network, otherwise you're asking for trouble. Firewalls block whatever you tell them to pretty much, including ICMP attacks, which are the most common when you're getting packeted. This can greatly reduce the risk of being packeted to death, but it doesn't mean that it won't happen. Nothing can fully defend against a smurf attack, but you can sure slow one down by having a proper firewall installed. There are several firewall types you can get, ranging from software firewalls such as Conceal PC Firewall, Freedom, or IP Chains. There are also hardware based firewalls and routers, the most prestigious of which are Cisco routers. Depending on how much money you wish to spend you can get varying degrees of protection. From packet routing, IP banning and looping to port protection, logging, and warnings. I have used several different firewalls, mostly software based and most are useless. For the most part they just log connection attempts. Although it is helpful to log, protection is still better. For your *nix based system I would recommend IP Chains and Port Sentry. Collectively they offer a great deal of protection. IP Chains routes harmful packets while Port Sentry logs connections and warns you of possible attacks. Port Sentry also negates most scans, stealth and otherwise.

Final Words

The last line of defense here are the services you're running. If you're running SMTP, HTTP, telnet, finger, etc., you're in deep crap, dude! You'd better get rid of every single one of those services, because they're all exploitable. Every service under the sun is exploitable, but these in particular because they're used so much more often and are far more likely to screw you rather than some of the other things. Let's start with SMTP. Simple Mail Transfer Protocol isn't necessary unless you're running an e-mail service on your box, so get rid of it if at all possible. Another risk (in addition to getting rooted through it somehow) is that of spoofed e-mail. It's possible to telnet to port 25 on a target and manipulate SMTP to send a fake e-mail to anyone in the world. Your best bet to prevent this is to block the service, or run ESMTP instead. HTTP is probably going to be a necessity if you're running a web server - just make sure that you have all the patches and security info available that you possibly can get because no web server, no matter how rare or how well coded it is, is totally secure. I recommend using Apache, since it's free and fairly stable. Just be sure to get all the patches and bug fixes for it. Telnet is a whole monster in and of itself. The service itself is secure, but not what it allows people to do. Having telnet open is basically an invitation to get your butt kicked, so close it off and don't allow shell accounts. Finally, as mentioned earlier, finger is a no-no. Anybody, even newbie wannabe hackers, can play with finger. It's basically there for one reason alone - to get you owned. Any buffer overflow will cause finger to give a user root access - it's the simplest type of attack. So make sure to block it out. If you want to get rid of these services, try editing /etc/inetd.conf and there are also some files in /etc/rc.d/ that you may want to have a look at too.

Hopefully after reading this you have at least a basic idea of how to secure your server. Although it does not go incredibly in depth, it is more than enough to keep most "kiddie" hackers out of your system.

Hacking QuickAID Internet Stations

by Durkeim the Withered God

There is nothing worse than waiting. I hate waiting to get food, I hate waiting to take a piss, I hate waiting for my paycheck, and I definitely hate waiting in airports. So there I was at 10 am, bored as hell, walking back and forth, until I discovered those mean looking Internet stations. I've seen a lot of different Internet stations around the world, but none looked as mean as these (they're like cubicles but made out of steel). Basically, in these stations you have a decent keyboard, a nice monitor, and an average interface. These are the QuickAID Internet stations (www.quickaid.com). In this Internet station, similar to all the others, you swipe your credit card, and for three bucks you can search for extraterrestrial intelligence on the Internet for 10 minutes. Oh well....

Finding the Operating System

This is always the best part of the entire process. I tried a few things: ALT-F4, ALT-ESC, ALT-TAB, Ctrl-Alt-Del, invalid characters, and so on. After overflowing the buffers by repeatedly pressing composite characters and special keys, I noticed the continuous Windows "ping" sound and the Windows desktop image in the background. That along with the "nice" polished icons is a clear indication of the evil operating system. As always, dumb developers chose Windows to program their applications. Just because it's easier to program in Windows it doesn't mean it's safer or better.

What Can One Do Without Paying?

In the beginning the access is very limited. We can only browse their web page using a stripped down version of Internet Explorer 4, send comments, and that's it. This obviously means that the machine has a permanent connection to the Internet.... Gooood.

Since I am such an ethical guy, I decided to save the brute force method (buffer overflow and keyboard/mouse crash) for a last resort. I decided to stick with the basics. So I started exploring the only gateway possible: their web page. As I expected, all the hot keys were deactivated. That meant no Ctrl-S and so on. The next step was to look at every document on their site to find a missing link. Before long I came across a zipped file inside the site. *Wrong move!* As soon as I clicked the file, our good friend, the unregistered version of winzip, came up. The machine was now mine.

Obviously the next step was to add a file to the zip files. I suggest that you add c:\winnt\system32\winfile.exe. (You all probably remember this as being the 3.1 version of Windows Explorer.) Then, just execute it after adding it. And voila. The system is now yours. You can edit the registry, change the settings, get the hot keys enabled again, navigate freely on the Internet, and, most important of all, you can disable that silly Cyberpatrol (unethical).

Browsing the Web

Using winfile.exe, execute c:\atcom\install\ATbrowser.exe and there you go. The rest is up to you. If you want you can even start an ftp server in their machines!

I'm submitting this article just to prove that Windows-based programming is wrong, bad, barbaric, buggy, morally wrong, and slow. Stop being lazy and program everything from scratch on a decent platform. You're not going to rediscover the wheel, but you'll have perfect control over everything! Control, my friends... it's all about control.

The Billboard Liberation Front

FOR IMMEDIATE RELEASE

CONFIDENTIAL -- DESTROY BEFORE READING

November 20, 2000- San Francisco, USA- The Billboard Liberation Front (SYM:BLF) announced a major advertising improvement offensive today, taking responsibility for the heroic modification of thirteen large-format billboards in Silicon Valley along the northbound US-101 freeway corridor between the Whipple exit in Redwood City and San Carlos exit.

The pro-bono clients in this campaign were all technology companies, with a sector focus on the endangered and much maligned "dot-coms". Billboards in the target sector were graphically enhanced by the addition of large-format warning labels, in the style of a standard computer error message, bearing the bold copy: "FATAL ERROR - Invalid Stock Value- Abort/Retry/Fail".

The BLF justified its actions under the emerging doctrine of Prophylactic Disclosure, citing recent examples of other industries that, through failure to self-regulate, eventually lost all access to the outdoor medium. "We love e-commerce", explained BLF Operations Officer Jack Napier, "and we really love outdoor advertising. We'd hate to see the New Economy go the way of Big Tobacco by failing to make a few simple disclosures". Citing the recent demise of e-tailer Pets.com, Napier pointed out the inherent dangers of marketing securities to children. "First Joe Camel, now the sock puppet- we're clearly on a slippery slope here".

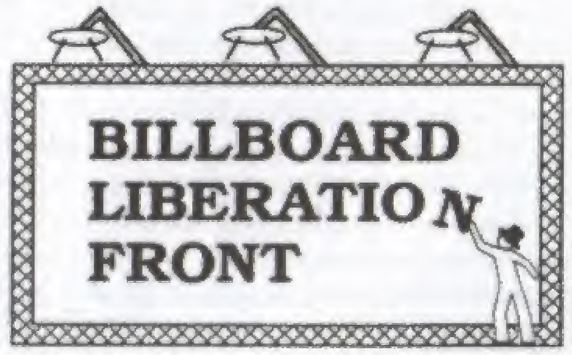
"The Internet bubble will not be allowed to burst on our watch", agreed BLF Information Officer Blank DeCoverly. "It's a very robust bubble, albeit temporarily low on gas. The fact is, these companies are drastically undervalued, and the investing public needs to be made aware of that. Would a dying industry increase its spending on outdoor advertising by over 670 percent in a single year? The naysayers are clearly falling prey to irrational under-enthusiasm."

Participating companies in the campaign included Internet pure-plays like E*Trade, Women.com, and Support.com, as well as "shovel-selling" high-tech stalwarts like Oracle and Lucent. The Pets.com sock puppet was not available for comment.

Founded by a shadowy cabal of understimulated advertising workers, the Billboard Liberation Front has been at the forefront of advertising improvement since 1977, adding its own unique enhancements to campaigns for clients including Zenith, Apple, Max Factor, Phillip Morris, and Chrysler.

For more information, please visit http://www.billboardliberation.com.

###



Computing With The Fabric of Reality

Chris Silva aka Sarah Jane Smith

This is an article in which I plan to describe quantum-based computers and their application for defeating public-key crypto.

Let's begin by describing basic quantum principle. Particles work in funny ways. It's believed that anything at the atomic scale obeys the laws of a very different type of physics than we normally see: quantum physics. Unlike classical physics, quantum physics deals with information and probability instead of physical forces interacting. For quantum-based computers all we really care about are particles in superposition, quantum entanglement, and quantum interference.

Particles in Superposition

A particle can have at least two different states, spin-up and spin down (or 1 and 0). That's all we care about right now. Logically, one would think that a particle with two states is either in one or the other. That isn't so. Under quantum physics a particle is in both (or all possible states, given its location) at the same time. That is, until the particle is observed, it's neither spin-up nor spin-down but both.

Quantum Entanglement and Non-Physical Communication

Quantum entanglement is when two interacting particles are in superposition. Schrodinger's cat is a good example. Say we have a particle in a chamber that either decays or does not. In that chamber there's a geiger counter that's hooked up to a device that releases a poison gas into another chamber that contains a cat. Since both the particle and the cat are in chambers we cannot see them. We cannot observe the particle to see whether it has decayed or not, and we can't see the cat to reason what happened to the particle. The cat, the particle, the geiger counter, and the poison releasing device are said to be in superpositional entanglement (or quantum entanglement). Only until we observe the cat, the reality where it died from the poison gas or the reality where it's still alive is our own. Any time before we observe things, the cat is both alive and dead. Although this example may not be too likely on account of the size of the cat and all, particles can become entangled in this way. In fact, particles can become entangled in such a way as to allow non-physical communication. Once in superpositional entanglement particles remain that way until observed, even if they move miles apart.

Say that we have two particles at 10:00p in superposition. At 10:10p we put both of them into a device where they are XORed (remember: spin-down=0, spin-up=1) so that the particles come out of the device as both 0 or both 1, or rather, since they're in superposition they're both 0 and 1 at the same time. Now we move them (in special containers that isolate them completely) to two labs: Alice's lab and Bob's lab. They both get their particles at 11:00p. Alice puts her particle into a device that changes it to a 1 without observing it (e.g. laser-cooling ion trap). Bob sits still and does nothing. At *exactly* 11:10.29p Bob and Alice observe the state of their particles. They're both 1! What this means is Alice communicated a 1 to Bob non-physically. Since their particles were in superpositional entanglement until they both observed them at 11:10.29p, one affected the other's probability of being 1 when Alice put hers into her device.

Quantum interference

Quantum interference is what makes most quantum-based computers possible. All possibilities are thought to exist in different universes and, on a quantum level, a particular universe with a particular possibility only manifests itself in our own when observed. There is no way to directly observe a possibility that is not our own, but we can do it indirectly! Imagine that you're standing on a cliff. There are basically two different things you can do. You can either jump off or walk away. You imagine yourself jumping off - you slam against the rocks at the bottom and die instantly. Since you don't want to die, you walk away. While you didn't jump off the cliff you imagined that you did. The frightening possibility of you slamming against those rocks interfered with you jumping off. This sort of interference of possibilities can be demonstrated with a photon. (Figure 1) A is a photon source that emits one photon, B and C are two detectors that can detect a single photon, and D is a semi-transparent mirror that, when only dealing with one photon, reflects or does not seemingly at random. Logically you would assume that both B and C have a 50 percent chance of detecting the photon because it went either one way or the other. While the results are the same, this is not what happens. When the photon strikes D it goes into a superposition of being reflected and not being reflected. Since both possibilities can be observed, they both try to manifest into our own universe. But the properties of D only allow one to. So there's a 50/50 chance of it being detected by B or C. Now, go to Figure 2. We've placed a photon-stopping plate in the non-reflecting path. Again, logically you would assume that the photon would have a 50 percent chance of being detected by B and a 50 percent chance of being stopped by the plate. And again, this is not what happens. But this time the results are not the same because of quantum interference. Because only the possibility where the photon is reflected into B is observable, only that possibility becomes our own. Therefore, there's a 100 percent chance that the photon ends up in B. Man that's weird!

Figure 1

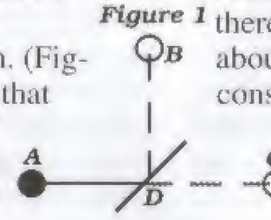
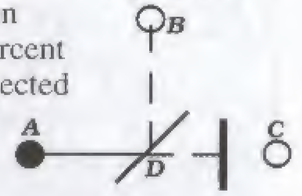


Figure 2

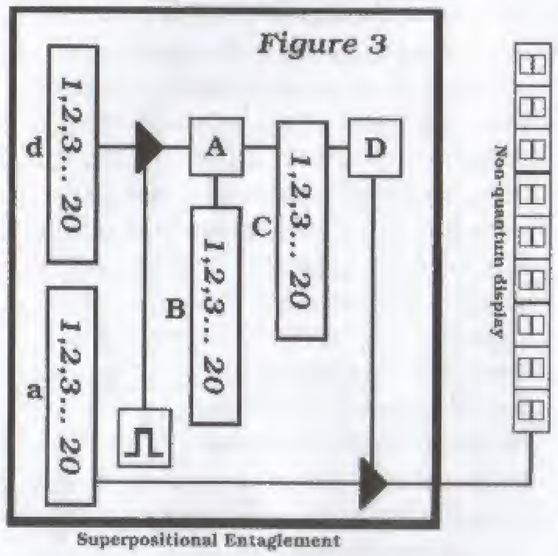


Better Things Will Surely Come Our Way

We have a million random numbers, each number being unique. We are looking for the address of number 10294. Under traditional technology there are only two ways one can go about finding 10294. One way is to consecutively check all one million numbers until we come across the right one. The other way is to do the same thing but divide

our workload by adding more checkers. Quantum-based computers do the latter, but in a very unique way. They divide our workload amongst checkers existing in different universes. As such, they have the capability of dividing work infinitely. So let's build one (Figure 3):

Classical memory cells (or bits) exist in two states, 1 and 0. Our memory



cells are individual particles and, as such, they obey quantum physics. Since we're not observing them (at first) they're in the superposition of 1 and 0. (A bit in superposition is called a qubit.) Recall that Alice transmitted 1 to Bob by changing the state of her particle. Bob's particle became 1 because it was physically impossible for it to be otherwise if Alice's was also 1 before observing it. That little trick of reality allows us to store multiple numbers in the same physical memory. Therefore, all one million 9 digit (or about 20bit) numbers can be stored in only 40 qubits (actually only 20, but we want the address too). If we changed the state (again, without observing it) of d0-19 to 0, d20 to 1, a0-a19 to 0, and a20 to 1 at the same time, we created a possibility for, depending on how you look at it, address 1 to equal 1. We can repeat this one million times until we've stored all our random numbers.

The classical design of our system is to let whatever is in d be sent to A during each clock. A compares its input with the number we're looking for, which is stored in register B. A stores the bit addresses that are shared between B and its input in C (e.g. if bit 2 of input and bit 2 of B are the same store 1 in bit 2 of C). D Checks C to see if all bits equal one. If they do, D switches on the gate to our non-quantum display which reads the contents of a.

This is what actually happens: During the first clock all possibilities stored in d are compared by A in different universes. Physically only one possibility can exist, so in that universe similarities between A's input and B are stored in C. Since C is directly related to switching on our observable non-quantum display, that possibility starts to interfere with others because it's observable. During the second clock, all non-observable possibilities stored in d are compared. In other words, d possibilities that do not have the same bit correlations with B as stored in C in different universes are compared. This is continued until there can only exist one possibility, we're looking at B in d, and that's when our display lights up with our answer! That is quantum computing.

Really Practical Applications

The great majority of cryptography systems, especially public-key systems, depend either heavily or completely on the difficulty of factoring large numbers. Quantum-based computers have the potential of reducing the predicted computing time of billions of years to mere seconds for factoring numbers of "secure" size. If such a computer were built, all public-key crypto would become insecure. So, let's build one:

The algorithm we intend to use for factoring is well known. The number we wish to factor is called N. We start off by taking a random number (a) between 0 and N. We then figure out a phase (r) by computing:

```
int find_phase(int a, int N) {
int tmpp, R[0xFFFF], r;
for(tmpp=0;;tmpp++) {
R[tmpp]=pow(a,tmpp)%N;
if(test_repeat_store_in_r(R, &r))
break;
}
return r;
}
```

After some time R[tmpp] will start to repeat itself, test_repeat_store_in_r returns true when this happens and stores the number of digits that repeat in r. Then we take the greatest common divisors (Euclid's algorithm) of (N,pow(a,r/2)+1) and (N,pow(a,r/2)-1). The result of this is the two factors of N.

Computing r under classical means is very slow. For increasing digits of N the computation time increases exponentially. The only thing our quantum computer is concerned with is computing r. The rest of the factoring can be done normally.

We have two registers in superposition, x and k. x and k are not prepared so that there exists the possibilities for x and k to be any numbers between 0 and pow(2,sizeof(int)*8). We then compute k = pow(a,x)%N (part of find_phase). After that we perform t=k, where t is some non-quantum register. Because pow(a,x)%N has the same return value for x+i*r, where i is any number, x is in superposition of all numbers that equal k. (Remember, we read k by t=k. K is no longer in superposition.) We are now ready to read x. There's a slight possibility that x=t. If this happens, we'll have to perform the operation again. If x!=t we have r=abs(t-x).

Now that we've found r in no time we can compute the greatest common divisors of (N,pow(a,r/2)+1) and (N,pow(a,r/2)-1) with a classical computer. This should take very little time.

The advantages of such a computer are obvious. Its potential for breaking public key crypto may be balanced by non-physical communication transferring secret keys about. Still, with *huge* increases in memory and theoretical infinite parallelism we'll be able to do amazing things.

My theory about the books *2001-3001* is that the black monolith was a small computer with the capability of simulating entire worlds. That LSD trip Dave had at the end of *2001* was him entering it. Now, is such a computer that far off?

SS MM SS

Politics

Politics

Dear *2600*:

I can't for the life of me understand why your magazine endorsed Green Ralph Nader over Libertarian Harry Browne. While I agree that Nader is a sincere man and infinitely preferable to Gush and Bore, a simple look at the respective party platforms will show that the Green Party is all about bigger, more intrusive government, and the Libertarian Party is all about freedom, no questions asked. In the crucial area of privacy rights, the Green platform is vague and poorly written; the bottom line is that *neither free speech nor the rights of the individual* are listed in "The Ten Key Values of the Greens" (www.greens.org/values/). On the other hand, the Libertarian platform (www.lp.org/issues/platform/freecomm.html) is crystal clear and leaves absolutely no doubt as to where they stand.

Ask yourself: do you want real freedom or don't you? The choice is clear.

Lisa J.

You've overanalyzed our message. If we wanted to endorse a candidate, we would have done so in a more obvious way. The cover of 17:3 was a collection of images that summed up the events of the previous months: H2K, the RNC, the treatment of the demonstrators, the rise of the Green movement and the questions they raised, the "threat" of a cell phone, etc. We don't care who you vote for and, as events have shown, it doesn't really matter anyway. And that is what you should be focusing your anger towards.

Dear *2600*:

I've been a long-time reader of *2600*, but looking at your most recent cover, I have to admit to being extremely disappointed that you would use your magazine to promote a particular political party. I'm all for encouraging people to support freedom of speech and all the other values that go along with the hacker ethic, but aren't you kicking yourselves just a little bit for voting Nader? Due to the closeness of the election and the fact that the Greens' views align far more closely with the Democrats than the Republicans, it's probably fair to say that Nader cost the Democrats the election. As a result, it looks like we're going to have a president who believes the Internet was responsible for Columbine. How do you think he's going to deal with Internet censorship issues? Gore, at least, understands technology. Just ask Vint Cerf.

Shame on you.

Ben Stragnell

If printing two words on our cover upset the status quo this much, we must have done something right. But what really should be offensive to most people is this arrogant attitude that both Democrats and Republicans have where they somehow think they're entitled to our votes. They're not. And the consequences of believing this as well as the absurdity of our current system were both aptly illustrated - in no small part because of those who didn't follow the party line. This was an unexpected accomplishment. And to berate these people for voting their conscience is simply unforgivable.

Dear *2600*:

Has anyone noticed none of the "protesters" in Florida were arrested? After the demonstrations at the Republican and Democratic National Conventions and the World Trade Organization meeting all resulted in the arrest of many people who were simply exercising their right to free speech and peaceful assembly, I would expect the same thing to happen in Florida. However, nobody was arrested even after one group of Bush supporters almost stormed the building where the recounts were taking place. Had this happened at one of the national conventions, the demonstrators would have gotten a life sentence. This tells me I only have the right to free speech and peaceful assembly if I am supporting the status quo, otherwise I will be arrested.

Chris S.

Now you're catching on. Another more recent example of the misuse of justice occurred in Philadelphia when drunken mobs smashed store windows and looted shops during a Mardi Gras "celebration." Here we had a violent crowd terrorizing people, causing massive destruction, and really screwing things up. Did they get held on a million dollars bail for ten days in prison like some of the demonstrators at the Republican Convention in the same city six months earlier? Not a single one of these rioters was even held overnight according to news reports. We see a distinct parallel with the way hackers are prosecuted - it's always the brightest ones who don't try to use their talents in a criminal manner who get the book thrown at them. The real threat to authority is knowledge, not crime.

Random Questions

Random Questions

Dear *2600*:

If cookies can be automatically downloaded to my computer, why can't some sort of virus be placed instead of a cookie? Don't you think that would be a way hackers and virus writers could get a virus into someone's computer?

MiStReSS DiVA

Cookies don't really work that way - they're generated by your computer and stored in a simple text file made up of single-line entries containing simple fields in ASCII. They simply can't be manipulated into binary code and your browser wouldn't try to execute it in any case. A far more insidious threat that Internet Explorer is prone to allows any file on your computer to be read remotely if its name and path are known. That's far more intrusive than anything cookies can do.

Dear *2600*:

Are you guys going to offer *Freedom Downtime* for sale on VHS or DVD? I would enjoy seeing it.

Frank R.
San Antonio, TX

That is our intention. We're doing everything possible to see that this happens soon.

Dear *2600*:

Hey why can't you hold a meeting in Newcastle-Upon-Tyne, England because you hold them in London and stuff?

Equinox

Technically, we're not the ones who hold the meetings. Various readers of ours do. And it's up to them to organize and publicize the meetings which we then list once they become established. More info can be found on our web page in the meetings section.

Dear *2600*:

Why does *2600* have a problem with the MPAA? They didn't make the DMCA. How come more pressure isn't being put on politicians?

Keyser Soze

There's this little lawsuit the MPAA filed against us that has probably swayed us away from their position. And they might just as well have written the DMCA themselves since they are among the DC special interest groups who are directly served by it. How much pressure is put on the politicians is completely up to individuals.

Dear *2600*:

You know, I think you guys have a lot of people buying your magazine. Why not make the magazine full size so more stuff could fit in it? Also, just so you know, your magazine is very easy to steal. How do you think I got my hands on this one? muhuahaha

Wax

We happen to like the digest size, even if it does tend to attract vermin. Stupid shit like this is enough to ensure that stores either keep us behind the counter or stop carrying us altogether.

Dear *2600*:

I am a subscriber of *2600*. I would like to know more about the cover of the Summer 2000 issue. Particularly I want to know who is the person in the picture in the fifth row and the second column?

muthu

As you may know, all of the pictures on that cover are scenes from our documentary "Freedom Downtime." The one you selected is one of only two that wound up being cut so either you're very observant or you made a lucky guess. This particular shot was of a manager at US West looking down on a picket line during a strike in 1998 in Denver.

Dear *2600*:

Does anyone know of any decent search engines one could use while being fairly certain that the search terms aren't being logged and/or being correlated with IP addresses? In these days of massive data mining/trend analysis techniques, one can't be too paranoid. ("Gee, this IP has a high density of flagged terms in its searches - time to break out Carnivore!)

EmptySet

There is no surefire way of remaining safe. Using anonymous proxies like www.anonymizer.com or www.safeweb.com will do some good but that won't protect you from anyone logging your keystrokes locally. Plus the anonymous proxy could also be compromised in one way or another or even be a setup if you really want to go for the paranoia gold. Perhaps the best way we can learn about such things as Carnivore is to trigger them more often.

Dear *2600*:

A colleague of mine recently went to a seminar in San Francisco regarding intrusion detection technology. These seminars are very popular now. His instructor, who claimed to be a previous security expert for AT&T (isn't everyone?) told the class to read *2600*. But the warning given was to buy it from the newsstand and not to subscribe, otherwise "you will get checked out." I asked him who would be doing the checking. But since he didn't have the insight or forethought to ask his instructor, it is unclear as to whether the alleged checker-outer is associated with *2600* or an outside agency (possibly government?).

So, in the interest of information gathering and because I am a subscriber, are you going to be checking me out?

Boneman

This would be unnecessary since we checked you out before you subscribed. That's why we made sure you heard about us and followed the plan by subscribing. Writing this letter, however, was not part of the plan and we will be taking corrective action.

Dear *2600*:

After getting my first issue of *2600*, I was bothered by something that I hope you can explain. On the second line of the mailing address label, I was surprised to see seven of the nine numbers of my social security number (in order) followed by seemingly random characters. I am not paranoid, and I could care less if "Big Brother" knows what I read, but I was curious about a few things. Why was it there? How was it obtained since it's not asked for on the subscription form? What were the characters after the number? With a rising amount of identity thefts resulting from social security numbers stolen from people's mail, it seems like a bad idea to even remotely refer to that number (especially on the outside of the envelope).

D'artagnon

We certainly agree that printing someone's social security number on an envelope isn't a very nice or smart thing to do. It's hard to imagine that you believe we would do something like this. The numbers on your label are comprised by your position in our database (anywhere from a one to five digit number) as well as the first three digits of your zip code followed by the number of subscribers in that area. Other letters and numbers indicate when you subscribed, when you expire, and your shoe size. Now enough with the paranoia.

Dear *2600*:

At the bottom of page 33 in issue 17:4, "Winter 2000-2001" is blacked out. At first I though it was a printing error unique to my issue, but everyone I asked

had the same thing. Could you please explain why it's like this?

haux

At best we can offer theories. Let us instead offer a promise that the problem has been fixed and won't ever happen again.

Dear *2600*:

I have been coming across this message regularly on my POCSAG decoding setup: "NEW PARIS TELEPHONE INC 02-1 ALARM 5ESS MAJOR ALARM". Then a few minutes will go by and I'll see another message which reads: "NEW PARIS TELEPHONE INC 02-0 CLEAR 5ESS MAJOR ALARM". Am I wrong or is this an ESS system sending a text message to an administrator's pager or something, warning him of an alarm being triggered?

And I would like to say thank you to Black Axe for the very informative article in 16:4.

Philter
Chicago

Your assessment is probably correct. You can see some very interesting things going by on unencrypted pager traffic. In the Netherlands a number of years ago a similar message was monitored that actually triggered a test of air raid sirens. We believe everyone should have access to pager information despite the fact that it's been made illegal by the same Congress that brought us the DMCA. The simple fact is that it's out there, it's unencrypted, and anyone can see it. It's ridiculous to think that outlawing the monitoring of a radio signal is a substitute for adequately protecting the transmitted data in the first place. We hope to see a lot more pager monitoring in the future so people can see firsthand how public it is.

Dear *2600*:

Let me start by saying that I think your magazine is great. The first time I read it was the issue before the current Winter issue and now I'm hooked. Your blatant honesty about things is great. Anyway, I was wondering about a rumor a friend told me. Supposedly the government blacklists anyone who subscribes to your magazine or anyone who buys it in the stores using a credit card. Now I have no problem buying it with cash, but I was wondering if the rumor is true or not. I'm sorry if this is an annoying question and you receive it often, but I wanted the truth. Keep up the kickass mag.

CyberInferno

Even if it were true, do you think they would tell us? If they did, we'd certainly tell you. But most importantly, if such a thing were going on, the best way to fight it would be to challenge it by getting as many people on those lists as possible. Even the hint of such oppressive tactics should not be tolerated. (And don't forget to wear gloves when handling currency unless you want your fingerprints in the central database.)

Ideas

Dear *2600*:

I am disgruntled with our phone service provider Qwest who charges us $1.90 a month not to publish our names and numbers. This is an unethical business practice and corporate sponsored blackmail. Therefore I am researching the phone numbers and addresses of some of their chief executives. I would like to know if you will publish this information on say a half page along with a request for them to pay $1.90 per month each if they would like the information removed from future issues. I think this will get the message across to those who feel they can bully the consumer who can't choose another provider due to phone company monopolies.

Phredog@Work

It would also get us in an amazing amount of hot water since the numbers are presumably unlisted in the first place. This little scam is nothing new to any of the local phone companies. You can easily get around it by simply listing your line under a different name. Then you also know when someone is calling you who is just reading your fake name in the phone book. Incidentally, the only reason phone companies get away with this crap is because they technically "own" your phone number and can change it whenever they want. We're just lucky the post office doesn't have the same attitude towards street addresses.

Dear *2600*:

Here's an idea. When somebody bitches about you guys owning "www.fuck(whoever).com", ask that company if they would like to buy the domain name from you. Let's say for like $10,000 or something. (Just make it cheaper for them to buy the domain name from you than to pay lawyers to take you to court.) If they agree, boom, you're $10,000 stronger against fighting the MPAA. Plus that's one less pissed off company breathing down your neck.

Reverand_Daddy

Plus we also get rid of those nasty things known as ideals. Don't you find it a bit disturbing for someone to sell their idea of free speech in order to have it silenced? Even if it were for a million dollars, it would be a pretty hollow victory. We should also mention that the moment you make such an offer, you are immediately perceived as having registered the site in bad faith and, in most cases, that alone is reason for you to lose the site.

Dear *2600*:

First I would just like to ask how you guys can complain about Gilian Enterprises. They obviously know everything and have a product that will stop every hacker on the planet dead in their tracks. What is wrong with you that you can't see that their vague references to things that sound technical make them industry experts? But I suppose if you are really tired of hearing from them, I will share a little trick I found on the net. (This was described in reference to credit card company mailers.) Once you get the spam and a valid contact address, you simply send them a nice response. "Thank you for choosing 2600 Marketing Consultants. We will provide you with a free analysis of the advertisement you sent us. We can offer these services for a competitive price (blah blah blah). Any future mailings will be considered a legally binding contract that you wish to employ us further." (include critique here) If they send anything again, you send them an invoice. May not always stop them and you might not get away with holding them to

it. But it certainly will discourage them. Until then, I urge you to buy their products. It is obvious their entire team needs the money to surgically reverse the recto cranial insertions they suffer from.

DragonByte

Info Hungry

Dear *2600*:

I recently spent some time with a long-time NYNEX employee who told me stories about PBX installations for the president at hotels in New England and during the Carter administration. Does anyone have any information about the presidential phone network? In the best interest of national security, of course.

Screeching Weasel

Any info we receive stays in these pages. We promise.

Random Fear

Dear *2600*:

Someone told me that they can search what I have on my computer. They said they could edit, delete, and add anything to my computer and all they need is to be online at the same time that I am. Is this true? If so, how do they do it? Is there a way I can stop this from happening? Please help me!

Brad

Bad security can make anything possible. We have no idea what kind of setup you have but if it's poorly designed, you could have all kinds of troubles. This is above and beyond any problems you might have at various online services who also may have security holes you could drive a truck through. Understanding your vulnerabilities is the fastest way towards understanding how they can be compromised.

Harassment

Dear *2600*:

I have an interesting story that everyone who enjoys privacy should read. I am a student at Northeastern University in Boston. Today I was visited by two policemen who wanted to talk to me about the content of web sites that I was viewing. They claimed that certain materials and or sites are flagged and that they know every web site I have been to. When I asked what specific sites were "flagged" they said I was being "evasive." When I asked if they will keep harassing me if I kept going to these sites they said "maybe." I still have yet to know the URL of a single "flagged site." I am wondering if this is true or not. I hate to think that my college tuition and money paid for Internet service is used to pay some person to spy on us. What should I do?

Nate

The first thing to do is find out just who these clowns are who visited you. What kind of "police" were they? Campus, city, state, federal? Or were they even cops at all? Once you have that established, demand to know what specifically they want and don't be afraid to raise a stink about this. Being a college student, you also have the advantage of possibly being around people who still believe in freedom of speech. Use that idealism to the fullest and don't be afraid to get others involved. Be prepared for any site that you may have visited to be made public - they may also try to make stuff up which is why keeping logs is a good idea. This kind of thing happens far too often and it's only by loudly challenging these people that anything will change.

Dear *2600*:

The other day as I was casually looking through a national newspaper I came across the headline "Give Up Potter Website, Film Giant Tells Girl, 15" and, like anyone else, I continued to read. To my horror, disbelief, and any other negative emotions you can think of, a 15 year old girl who owns the site www.harrypotterguide.co.uk/ received a threatening letter from, yes, you guessed it, Warner Brothers stating that if she didn't hand over the domain to them she would be liable for legal action against her. The site itself does not claim to be anything but an unofficial fans' site and even links to the official Warner Brothers site. What makes it worse is that before creating the site, she wrote to the author of the book who replied, "Thank you very much for being such a Harry Potter fan."

Sam 'E'

You can learn more about this at www.potterwar.org.uk.

Dear *2600*:

Since I have free time now, I figured I would write about the severe injustice I suffered at my local high school last year. As a reader of your magazine, I acquired knowledge of the back doors, loopholes, and security issues of Windows NT. Knowing these exploits, I attempted to educate and help the technology director of the school by showing him a couple of possible security issues he might have. I figured that would be the right thing to do, seeing how there are many vandalistic children who take pride in "messing up the computers" at school. Well, apparently knowledge is illegal. I was immediately suspended from the computers, banned usage of them for over a year, and given warnings and detentions by my dean. For what? Just for trying to aid someone? I do not blame this on my schooling system as much as I do the person who initiated my injustice. Had the technology director asked me to kindly not show him what I had known, that would be a different story. But he insisted that he should see the exploits. Over time, I have protested to my dean and regained access to the school's computers. But whenever I do use them, I am under the strict watch of the admin. I do hope people learn from this and realize that sometimes help isn't appreciated.

RagnSep

Dear *2600*:

We have never been Mitnick fans and have always distanced ourselves from his controversy. But what we have just seen disgusted us and made our blood boil. It seems that Mitnick could possibly get into even more trouble for something he didn't do. While trying to determine the source of conflicting news stories about the recent (1/25/01) Microsoft DNS breakdown (was it a technical fuck-up, a genuine hack, or ass covering?), we ran across an interesting, yet disturbing, picture on the

home page for Fox News.

The graphic is a collage of computer-related pictures and symbols, plastered beside Fox's Microsoft headline. The most noticeable feature is the right half of Kevin's mug (the chubbier, younger, pre-trial Kevin), strategically placed to give the story a mysterious, menacing appearance. It is shocking and outrageous that his face is used to adorn a news story he has absolutely nothing to do with. It's one thing if the story delved into past hacking incidents and used Mitnick as an example, but nowhere in the story is Mitnick mentioned or implied! Why must his picture be associated with this, especially since at the time of the incident there were conflicting stories between rival news agencies attributing the Microsoft DNS error to either a technician entirely goofing up with no mention of attack (Reuters), or a massive DoS attack after the goof was fixed (AP). Nobody can get the facts straight!

This kind of bullshit could crumble the fragile freedom Kevin currently possesses. If the "wrong" people see this web page from a supposedly "reliable news organization" and start asking questions, they could decide to place him back into prison for no reason whatsoever. How many others out there are going to assume that he's involved with the Microsoft fuck-up just because his picture is there? It angers us that some semi-creative artist with a G4 and Quark could unknowingly ruin this man's life all over again. May Fox News and Rupert Murdoch burn in hell for a thousand eternities. I am registering foxnewssucks.com right now and will cache the webpages there.

He did his time, he received his punishment, he needs to be left the fuck alone.

MajickMutex
Jenn

This is really par for the course as far as the media and Mitnick are concerned. But we're glad this instance opened your eyes. It's also somewhat ironic that they got that picture from the 2600 site without asking us. Now imagine if we did that to them.

Dear *2600*:

I have two problems: My principal suspended me from school for posting flyers about *2600* meetings in the halls. Do you have an explanation I could give to him and the tech guys so I can get my Internet privileges back along with respect from the tech guys?

My second question is this. Every time anyone in my family calls anyone we hear a dial tone in the background and then the lady that says "hang up and try again" comes on. Do you know how to fix this?

KNP

You don't owe your school an explanation - they owe you one. Like how posting a flyer is a reason to suspend someone's Internet access. We could tell you to try and explain the concept of 2600 meetings, how they're open to everyone, how we don't commit crimes, how it's all about learning... somehow we think it would fall on deaf ears.

As for your phone problems, it sounds like a crossed wire. You seem to be picking up two lines but only getting out on one. The second line times out and gives you the off-hook error. We suggest trying this from the point where the phone line comes into your house. If you notice the problem there, then it's the phone company's fault and they have to fix it. If you don't, something is wrong with the wiring inside your house.

Dear *2600*:

My school, Baylor University, has recently decided to attack the non-official student publication, *The Baylor Review*, for using their name. They contend that we will cause mass confusion and are threatening legalities unless we relinquish the name and the domain (www.baylorreview.com). To me, all of this is just stupid. We are non-profit, they have allowed us to distribute on campus since November of 2000, and this comes after we published something that may have *gasp* offended or embarrassed some of their professors.

Since you guys have been in very similar positions (at least with domain names), I was hoping that maybe you could give me some pointers or advice.

Corv

It's an intimidation tactic and they will only look bad if they pursue it. Since you are a publication, you have an immediate advantage in being able to reach people. We suggest that you publicize this as much as possible until the university backs down. Precedent is also on your side - The Dartmouth Review has existed for ages as a non-affiliated publication for Dartmouth College. As long as you're not pretending to be something you're not, such as a department of the school or an officially sanctioned publication, you're in the clear.

Cluelessness

Dear *2600*:

I just wanted to write to say I'm miffed. No, fuck that, I'm *pissed*. I'm an Internet consultant and I recently took a contract at a new company. Now, like a lot of consultants, I work off hours. Here I was sitting at the office in the wee hours of the morning waiting for a friggin' server to reboot and I thought, "Hey, I'll go see what's new at 2600.com." Lo and behold, what do I see on my screen? A message telling me this is a non-business site - "reason: criminal skills". WTF? Apparently, whoever set up their "nannyware" doesn't have a clue. I make it a point to hit your URL at least 20 times a day, just to make a point to those who read the logs. Maybe someday we can reach all the misinformed and uninformed, but that's apparently not today.

Have any of your other readers seen this?

Parin

Far too many.

Dear *2600*:

Our Verizon account is useless because they block access to our own SMTP server. When I signed up for a business account with Verizon to provide dial-up access for our sales representatives, I was told that we could use our present e-mail server over the Verizon dial-up service. Now I find that this was not true. According to the Verizon technical support supervisor, Verizon intentionally prevents customers from accessing any SMTP (outgoing mail) server other than those owned by Verizon. The excuse for this action is to prevent "spam" e-mail messages, but the result is that competing services are prevented from operating over dial-up Internet connections provided by Verizon.

Randy Ford

Dear *2600*:

Having been a fan of this publication for quite some time, I could think of no better way to show my support than to purchase a tee shirt from 2600.com. I chose the blue box design and have worn it with pride. Recently however, I've noticed that when I wear it in computer stores I receive nothing but cold stares and dirty looks, almost as though they suspect I'm going to rob the place! It's like they're profiling me because of the shirt I wear, which is a shame considering *2600* is so strongly against criminal activity. In fact, one gentleman I met at the mall was surprised that I had the courage to wear such a shirt! I was about to discuss the magazine with him but he seemed to think that we would be arrested just for mentioning it. I honestly believe this may be a reason why certain people don't want to wear such clothing. All I can say is that we need to let people see we're proud of what we are and what we stand for. No matter how many dirty looks I receive, I will continue to show my hacker pride and not let these sadly misinformed individuals get me down.

Screamer Chaotix
Connecticut, USA

The only answer to this kind of ignorance is to make more shirts.

Dear *2600*:

Recently my mother passed away. I went looking through the family photo album for a picture that I could enlarge to display atop the coffin during the service. I found a picture that I really liked and everyone felt really showed her well. I took the picture down to the local Target to use the nifty little Kodak image processor. As I was laying the picture onto the scanner bed, an employee came by and told me that I could not enlarge that picture. The picture was taken at a studio, therefore I couldn't make a copy. Since the picture was dated 1986, which would have made me four at the time, I went and asked my father where the picture had been taken. He was sure it was a small local studio that has since closed down. So now I had a picture that my mother paid money for, but couldn't have enlarged and displayed at her funeral 15 years later because of copyright. So I went to Kmart where nobody cares and used their Kodak image processor to do it. Copyright, or at least the current way we have it set up, is bullshit.

SellOut

Observations

Dear *2600*:

I have noticed as a reader on and off over the last few years that *2600* has become more of a political and social platform, in certain aspects, than a technical forum. The Fall 2000 issue was good, more techie articles I felt. Don't get me wrong, I know what the magazine has been through of late, but it is hard to get my new issues every few months and find it filled with articles about what court cases you are going through and reading about kids in high school who are getting busted by cranky old English teachers and such when I am expecting information for these kids and myself about computer and phone systems. I guess my question is: Where do you see the magazine going? *2600* is the place I go to get new ideas about tech issues that are more edgy as well as new ways of looking at them. I hope that isn't lost in these philosophical and boringly accusational arguments. I really want to impress that I do want to support *2600* in the court cases etc. but I want a tech magazine as well.

C....

We'll make you a deal then. We will continue to try and print edgy technical info that others are afraid to touch if you help us fight for a society that will see this as a good thing. We would like nothing better than to be able to print articles without having to worry about which megacorp will come after us next. But as long as that keeps happening and as long as freedom of speech and association are punished instead of embraced, we're going to have to fight back, in these pages and in other forums. If we lose, you likely won't have anything at all to read.

Dear *2600*:

While reading an online article about your recent court ruling to remove linking to DeCSS code, the article stated that linking to the material was considered illegal. This is what caught my attention. Now not only distributing this code is illegal; but the mere act of inserting a link into a web page to this information is illegal. It would be like you asking me where you could buy a gun. I tell you Dick's Sporting Goods and then you kill someone. Am I responsible for any wrongdoing (keeping in mind that I didn't provide you with the gun but only the information on where to buy one)? It seems to me that the ruling is extremely unfair and unconstitutional.

31337

We prefer to avoid gun analogies almost as much as house analogies. What we need to remember is that we're talking about speech, something far more valuable - and powerful - than any weapon. Many reasonable people are sickened by the proliferation of guns in our society. But to see speech as a threat - that requires a distinct hostility and fear towards the openness we've always been taught to value. You don't need an analogy when the actual event is so blatantly wrong.

Dear *2600*:

I was doing some research on different computer laws and came across an interesting section - the House Committee Report on the Copyright Act of 1976, page 54, states that the term "literary works... includes computer databases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves." Now if a computer program (DeCSS more specifically) falls into a similar if not identical category as a literary work then it should stand to reason that it would be protected by free speech as well.

Kyle

Dear *2600*:

Have you ever had a traffic ticket? Well, I for one

have, and a lot of my friends have as well. I have also found a major flaw in the Ohio computer systems that control the "points" you receive when you get a ticket. This may work in other states, although it has not been tested. Now here's how it goes. If you are over 18, then this pertains to you because minors have to appear in court. So you get your ticket, let's say for $100.00 to make it simple. Now you have chosen to pay by mail. You write the check for $105.00 (accidentally - wink wink), then you mail it in right on time. In a few days you will receive a check for $5.00. Don't cash it. This will show the computer that you paid, but it won't actually be finalized so no points will be put on your license. I have had several friends try this and it worked for them.

~otacon~

It's somehow heartening to think of people all over the country rushing out to get moving violations so they can test out this theory.

Dear *2600*:

Something rather interesting I came across on the Internet: If you go to the Radiohead site (www.radiohead.com) - make sure you go completely into the site - there is a link to the *2600* Secret Service page. It is under "trapdoors". Go to the one that says something about dots. I think it's great that word of you gets around. Then again, no reason it shouldn't. Keep up the good work and don't let those corporate giants try and bully you.... The bigger they are the more they bitch... err harder they fall.

RevZer0

Dear *2600*:

I was poking through the registry in Windows and cam across an interesting key. Go to "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion" then look for "DVD_Region"="1". I don't know if changing it will allow you to watch a different region code DVD. I don't have a DVD installed on my computer.

Three

Dear *2600*:

I liked the Fall 2000 cover. Nice touch with the handcuffs!

Mad Pyrotechnologist

The Philly police really deserve all the credit.

Dear *2600*:

Everyone has responsibilities in life, like it or not. First, let me tell you about mine. I work for one of the largest consulting firms in the world. When first hired, I had very little job security due to the fact that I was well known as a hacker. Over the period of two years, that has changed. Most of the people I work with are now extremely interested in non-malicious unauthorized security audits. *2600* articles are now everyday conversation material. I feel I have done my part, relative to my responsibility, to clarify to the people in my scope what the word "hacker" really means. You, however have a much larger scope and have voluntarily assumed the responsibility of being the voice of the hacker community. Why then is it that all you can do is piss and moan about the bad connotation the word "hacker" has received? We are hackers, not criminals. It is your responsibility to make this known on the global level. I therefore respectfully request that you stop pissing, moaning, and trying to play martyr, and voice to the world what a true hacker is. We will be extinct sooner than anyone realizes if we don't take our name back from the irresponsible, adolescent, power-tripper wannabes who just want power and a free ride on our coattails 'cause they literally can't hack it.

(The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorized.)

Trigga Bistro

Well, you've got us thoroughly confused. You want us to fight for the word "hacker" but not complain when it's misused? We'd sure like some specifics on how such a thing can be done. And keep in mind that we have access to, at most, four dimensions.

Dear *2600*:

Please spare us your bleeding heart commentary on the RNC protesters in Philadelphia this past summer (as mentioned in the editorial in 17:3 and again in a letter from Prehistoric Net Guy in 17:4). I work in Philadelphia and witnessed it firsthand. I saw a chaotic group of drunken douche-bags with no political message or common cause who showed up simply to vandalize our city. The "puppet factory" also had a nice supply of bats, pepper spray, and other goodies that Prehistoric Retard forgot to mention.

Point in fact: One of these morons (probably one of the same type of geniuses who releases an e-mail virus on the web for kicks) picked up a newspaper machine and launched it into oncoming traffic for no other reason than to have a laugh with his buddy. A sole Philadelphia police officer instructed this idiot (in a calm manner no less) to return the machine to its original spot. At this outlandish request, the protester picks up a bottle and whacks the cop square in the face. When the cop grabbed him, another protester came over and the two proceeded to kick the crap out of the cop until they were finally scared off by a group of citizens and approaching police. The officer never drew his gun or nightstick, despite having every right to do so (I would have shot the assholes).

The Philly cops remained calm and violated no one's rights, despite what the liberal news media tried to portray. I have no sympathy for any of these opportunistic "protesters" and they did not win any citizens of Philadelphia over to their cause (whatever that cause was... unrestricted vandalism perhaps? Public loitering and drunkenness? I am still trying to figure it out.).

If you are going to make a statement, at least make it accurate. All these charlatans who were arrested got what they deserved. And no one was abused by the police... period.

Your Mom

Well... thanks for setting us straight. Now if we could be permitted to steer your ship a little closer to Earth for a moment, we'd like to ask a couple of things. If something as you describe were to happen to a cop, you can bet a hundred other cops would have immediately converged on the scene - it was a demonstration after all and they weren't exactly isolated. In addition, with the vast number of cameras and media around, there would have been multiple camera angles of this incident. The "liberal news media" were most definitely not sympathetic to the demonstrators so why didn't we see this event over and over? And let's for a moment assume that it even happened. You seem to have trouble distinguishing drunken idiots from intelligent protesters. How do you know these people had anything to do with the demonstrators who were arrested and held in prison for ten days on a million dollars bail? (And incidentally, virtually all charges wound up being dropped or dismissed when no evidence was presented.) Why were none of the Mardi Gras vandals and hooligans treated as harshly? Where are your criticisms of a truly drunken mob intent on destruction? We realize that civil disobedience can mess up your schedule when protesters block traffic on your way to work. But it takes guts and commitment to a cause. That should be respected whether or not you agree with their position. You had a chance to interact and learn something from people with a different perspective. Instead you chose to reinforce your stereotypes and spread venom. It's your loss.

Dear *2600*:

I just wanted to tell you that the paper you use for your mag is some of the best smelling paper out there.

tnt419

We try.

Dear *2600*:

I was intrigued with this quote and thought it might interest everyone. "The search for static security - in the law and elsewhere - is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts." -William O. Douglas (1898-1980) U.S. Supreme Court Justice

Wow.

zerolemons

Dear *2600*:

In the wake of what will no doubt be the end of the first of many chapters to come in the DeCSS case, I think it's great that you guys are standing your ground. Contrary to most of the suggestions you've been getting, rather than finding a way around the parameters set by the MPAA, you're going to keep fighting for what you believe is right. Thank you.

noire
Colorado

Dear *2600*:

Radio Shack is now selling the memory tone dialer for $4.97 if you can find it. Yes, they are discontinued so no more can be ordered. If you don't get one, they will basically be thrown out, so dumpster diving is also an option.

Eric

Dear *2600*:

Regarding "computer" * 6 = 666 and "hackers" * 40 = 2600, even better: Take the ASCII code (A=65, not A=1 as in the above examples) from "WILLIAM H. GATES III" and divide the sum by two.

Oh, we knew it....

kju

Dear *2600*:

Just wanted to let you know that someone on Napster is sharing the H2K mp3 files that you have on your web site.

almightycoop

That's why we put them up on the site, so people could trade them freely.

Dear *2600*:

I had just bought the 17:4 issue and never really had time to read it. I took it to school and began reading through it. I saw the article on MSCE and gave it to my friend who was talking about how he wanted to become a MSCE. He in turn went out that night and bought the issue. The next day he showed it to our graphics design teacher. After he told me this, I thought to myself, "Great! There goes my high school career." Turns out the teacher was pretty cool about us having it. He had read the article on hacking NT. He even thought it would be a good idea to try it. So guess what!?! He showed the article to my programming teacher, who happened to be the head computer guy at our school. Now I'm in deep shit, right? No. My teacher thinks that reading the magazine would be one of the best ways to learn to program! Now he is getting a subscription for himself and maybe a subscription for the school. Add a few more pages and your magazine could be a text book for a classroom.

Biohazrd51

Dear *2600*:

Greetings. If you don't know, Jello Biafra's H2K speech is included in his newest spoken word album. "Become the Media" is a 3 CD set that you can pick up at www.alternativetentacles.com. There's also a bunch of kick ass pieces against globalization too. No, this is not an ad, but I think that a lot of hackers might be interested in checking it out and also becoming more involved/knowledgeable about the anti-globalization movement. Best wishes and good luck with the appeal! Solidarity.

Xian

It might be a good idea to rush down to Walmart and demand that they stock this. Don't hold your breath.

Dear *2600*:

Greetz from Germany where I just had my final exams in high school. English, biology, computer science, and crypto were the main topics of the five hour long exam. We had to decrypt some texts and find keys. I thought putting on the *2600* shirt with the crypto theme would be totally Zeitgeistish so I put it on during the exam. My teacher had to check if the info contained on the shirt would help me in any way. He found that it wouldn't and asked me where he could buy one of the shirts.

zeitgeist

Dear *2600*:

Let me start off by saying that I understand that the

extent of your involvement in so much legal controversy must require an immense amount of money. Of course the EFF cannot cover everything, but I am sure that by lowering the price of *2600* you would get a lot more readers. $7.15 CAN is far too expensive, and everyone with at least a little common sense knows very well that your production and distribution costs are not that high.

hemlock

First off, we're not jacking up our newsstand rates to raise funds for the lawsuit. Our price has been the same for two years and our subscription rate is the same as it was all the way back in 1989! As for the Canadian dollar, it converts to less than 65 cents of a US dollar. That means you're actually paying less than people in the States. For a long time we were selling 2600 at the wrong exchange rate and we actually wound up owing our distributor money for sales. You're welcome to use this common sense of yours and try to do what we do for less money without any advertising. We think you'll find that talk is about the only thing that's still cheap.

Dear *2600:*

Hey guys, just a head's up - it looks like somebody has caught on that corporate evil exists in not only the technologies industry, but the airline industry as well. I found that www.fucknwa.com graciously points to Northwest Airline's web site, www.nwa.com.

Weez

Dear *2600:*

I was wondering if you guys have looked into a program called ASF Recorder. It's described as enabling someone to download streaming content in Windows Media Format to their hard drive. The resulting files will be in ASF format and can be played with Windows Media Player and derived tools. You may call this the "DeCSS" for Windows Media.

patrick

Dear *2600:*

Whether or not I view sending MP3s over the Internet as just harmless sharing, I don't believe laws such as DMCA and the ruling on Napster are good decisions. One of the most fundamental things a law should possess is the ability to be enforced. Without it, the law is just a collection of words on paper. This is the situation with DMCA and the ruling on Napster. You *cannot* and *should not* even attempt to restrict the Internet or computers in any way, except maybe the Computer Fraud and Abuse Act (realistically speaking, we probably do need that law). Unless the government hires thousands upon thousands of computer experts to constantly scan the entire Internet for "illegal" files, considering how dynamic the Internet is, they would have no way in hell of ever enforcing that law, rendering it useless. It is a bad law.

rootx11

Dear *2600:*

I was looking around in my new copy of issue 17:4 and noticed on page 44 the statistics of the magazine's subscriptions. Is it true that there are only 5,680 subscribers nationwide and only 75,000 issues sold per quarter total? This is disturbing. With such a long history of publication, I would have thought that more people would support your (our) causes by subscribing or, at least, buying the magazine. Perhaps I should get more "Free Kevin" and "Stop the MPAA" bumper stickers to place on my car. I should mention, also, that I like the new format of the web site.

Sir_Poet

75,000 may seem small to you but to us it's huge. Considering that our first issue was sent to a couple of dozen people, it's almost frightening how far we've come. Of course we can always try to reach more people but we find it incredible that we've made it this far.

Dear *2600:*

I don't know about the rest of the world but Verizon has an ad campaign going in Pennsylvania, stating "Keep Verizon together for the good of Pennsylvania."

shader

That sounds like a veiled threat to us.

Dear *2600:*

I was sitting down watching *Romeo Must Die* after a long day working and needing to unwind by watching some serious ass getting kicked. Anyways, about halfway through the movie, the main character picks the lock to the apartment of his murdered brother. Why is this important? The number on the door was none other than 2600! I don't know if the studio is one of those who sued you or not so I don't know if there's a hidden meaning.

gan0n

Sometimes a number is just a number. But who's to say?

Discoveries

Dear *2600:*

I recently found this massive computer thing a local company had next to their dumpster. I figured they didn't want it anymore and that it would be interesting to pull apart. When I got it home, I decided to plug it in to see if it worked and it seemed to be OK, making a few beeps and hdd light flashes. I think it's some sort of telecommunications or networking device but it's very old looking and has no means of connecting a monitor or keyboard or anything. It's called a Telemetrics System 1XXX and there is another sticker that says Telemetrics S600. I have tried their web site but can't find any info on this beast, as they only seem to give out technical info to corporations by an application. They also don't call themselves Telemetrics.

So to cut a long story short I was hoping you would be able to point me in the right direction to find some documentation about it or shed some light on what it actually is.

Kal

We'll ask around. It would have been helpful if you told us what name they actually use instead of Telemetrics.

Dear *2600:*

I found these exact instructions while at my local TV shop last weekend.

"Instructions To Convert Orion DVD Player To Region Free Status

"1. Connect DVD to your TV.

"2. Simultaneously press and hold down OPEN, STOP, and FAST FORWARD buttons on the DVD player.

"3. After a few seconds a menu will appear on your TV screen.

"4. Using the arrows on your remote control, select Region Number and change from 2 to FREE. Press Select on remote control.

"5. Change Colour System Setting from Manual to Automatic and press Select.

"6. Go to EXIT and press select.

The DVD Player will now play all region discs."

These instructions apply only for Orion Model D3001. Thought you might find them interesting. I haven't tried them out but the shop claims they work.

Robb
Ireland

Dear *2600:*

I was playing around on my phone dialing numbers with Verizon prefixes. I sort of hold a grudge against Verizon Wireless because of how they fucked me over into a contract. They were claiming "free nights and weekends" and even had the signs but when I spent about 1000 minutes on my weekend phone, they clarified that free only meant 800 minutes. Fucked over and dealing with it while bound in a contract, I found out a number they use for directory assistance. This is it: Dial "812.454.0012" and you are connected to Verizon's nationwide directory assistance. They also will connect the call for you automatically. Your ANI will come up as "812.454.0012". Cute, huh?

Splices

Memories

Dear *2600:*

Can you remember the times when you were standing at the payphone, hacking VMB's just to have a box to pass around (with the same h/p info as all the other VMB's out there)? How about traveling at speeds of 2400 up to 14.4 to a BBS with one node to download something that was 800k and still took a half hour! That did not include the time to get through to the BBS, due to busy signals! Amazing - now we complain that our cable connection is slow.

This was true hacking. When the world was truly "underground," trading good info to each other. Calling cards never died, no such thing as "trunk tracing." Oh yeah, "Operator, can you place this 1-800 number for me, I have operator privileges." Good times and we loved it. How about the bridges? They never died and we all got along, trading our info for the good of each other, no one else, just our own little clan.

I cannot remember how many "h/p/a/c" groups that I was a member of, only that I loved being in each and every one of them. And you know what separates "us" from the rest? The fact that "we" did this for kicks, not for money. We wanted the power and we got it. No one was a rat. We were all a family.

I loved those times and I thank everyone for being a part of it. Because of this wonderful hobby, I have succeeded in my goals.

Stevie B a.k.a Blue Lightning

Things are never the same. But in other ways they are. The years you describe are undoubtedly beyond the point where others would say things changed for the worse. And what's happening right now will one day be described as the good old days. It's up to all of us to see that the magical spirit that has been a part of the hacker world from the beginning is preserved and respected. There will always be people who get it and as long as they exist, there's hope.

Fighting Back

Dear *2600:*

After reading the Verizon article in your summer issue and the subsequent letters in the fall issue (not to mention the ridiculous letter from CBS), I decided I could put a domain name I was holding onto to good use. I would like to extend an open invitation to your readers to post a page of protest against whomever they like on sucksdonkeyballs.com. Of course, the effect wouldn't be complete without subdomains so all pages will get their own. Who wants to be the first to post verizon.sucksdonkeyballs.com?

Scott

Dear *2600:*

I wanted to contact you to inform you that your efforts are not going unnoticed. I am a graduate student in San Antonio earning a Masters in Fine Art. As of today, my new work will be up in Gallery E, a campus gallery run by the grad students themselves. I have signed up for this space and will have it for the next two weeks.

The reason for me contacting you is because my new work consists of the issues at hand here with the MPAA and DeCSS. I followed the trial over the course of the summer and upon learning the verdict felt that I must do something. The piece itself is called "DeCSS." Exhibit A consists of 12 binders containing the entire court case as displayed on your web site. Exhibit B consists of the actual source code for DeCSS, obtained long before this whole disaster struck. Exhibit C consists of four t-shirts with the words css_descramble.c written in the center and hung on the gallery walls.

rene gonzalez

Dear *2600:*

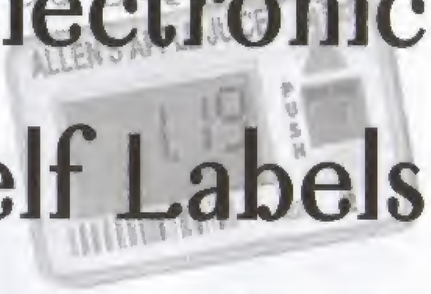
Last night the officers of MGN (Metropolitan Gender Network), a group for transgender, transexual, drag kings and queens, resolved to send *2600* a message of support for your fight with the MPAA about the DVD decryption code. Our struggle is inextricably tied to the battle for freedom of speech. We wish you luck in your court fight.

Marina Brown (MGN)

We haven't gotten support from every walk of life imaginable but we're getting pretty close.

Letters continued on page 48

Secrets of Electronic Shelf Labels



by Trailblazer
traiblazer@usa.com

While the supermarket experience is probably taken for granted by most of us, some will nevertheless notice that these places are technologically evolving. Computer-based cash registers, laser quality receipts, and commercials running on flatscreen monitors are all commonplace in today's supermarkets.

Remember those clunky guns that spit sticky price tags, allowing even the slowest stockboy to price a case of canned soup in seconds? Well, they've disappeared, too. In most of today's supermarkets, you'll see a laser-printed label placed on the edge of the shelf. Some supermarkets have gone a step further and introduced electronic shelf labels (ESLs). Through some social engineering during some late night shopping, I've learned a little about these things and would like to share this information. Hopefully you'll find this technology as fascinating as I do.

These ESLs are simply small plastic panels with an LCD display, prominently fixed to display a product's price on the edge of the store shelf. There are several companies that manufacture these products, but in my area's supermarkets there are two chief vendors: Telepanel Systems and Electronic Retailing Systems International. Their price tags come in various shapes and sizes, sometimes with one LCD display and sometimes two. In my local supermarket for instance, smaller items like spices and condiments have small displays; larger products like paper towels have larger tags. Some even have hidden buttons that display additional information (product UPC codes in my limited experimentation) when pressed. They're pretty rugged and if you've ever worked in a supermarket you'll know why. These things need to withstand runaway shopping carts and bored children's busy hands. I would guess they're also water-resistant for obvious reasons (or should I say raspberry jam-resistant)!

I've tried removing one of these tags from the shelf and it was tough. The shelf edges were slotted to house the tag snugly. Once I did remove it, I noticed the tag was powered by a wafer-type watch battery in the back. I removed the battery, awaiting the obvious effect of the LCD display going blank. I replaced the battery however, and the original price returned. How?

The electronic price tag system is quite sophisticated. Imagine the supermarket as a giant LAN, with each price tag being a node in that network. Each tag communicates with a server somewhere in the back office. This server receives a feed from a database running on the supermarket chain's main

server, presumably located at its headquarters. So price changes can be automated right down to the shelf. For example, a supermarket bigwig at the headquarters decides the price of Jell-O needs to go up. He makes that change in the database, and that change is pushed to each store's back office server which then sends that update to the label. Voila, the price has changed on the shelf, no price gun required. That back office server is obviously part of the POS (point of sale) system, so you know you'll be paying that new price as the clerk is ringing you up for your Jell-O.

The means of communication between the price tag and the back office server is even more remarkable. In my supermarket (an Electronic Retailing Systems customer) this communication is wireless - the labels communicate with their server via RF! Cellular transmitters are mounted on the ceiling and transmit via a 2.4 GHz spread-spectrum frequency. Price changes are distributed in this way. When the label receives the message, the display is updated, showing the new price.

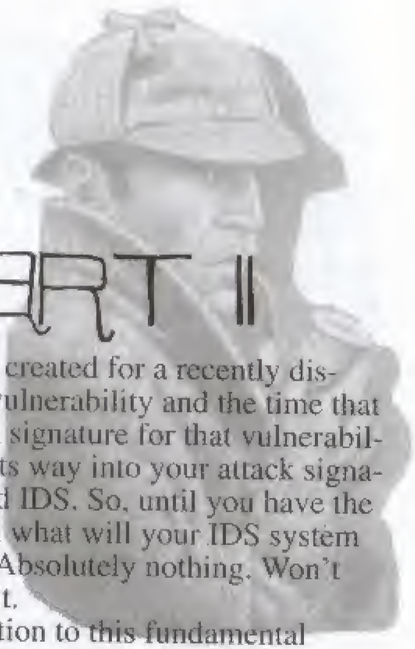
Though I'm not sure how, RF communication occurring between each label and the server is two-way, and it resembles a TCP connection. Each label has a unique hex address (it's printed on the side), and it's constantly "listening" for messages containing its address from the server. So when the server has a price update for a product, it transmits the price information as well as the address of the label for which that update is intended. The label receives this data, then sends an acknowledgment message upon receipt. If the server does not receive this message, it sends the price update again until the label replies. I'm assuming the RF occurring is very low power - I counted three or four ceiling transmitters per 50 foot aisle. I would also reckon the FCC would complain if we were looking at anything more than a fraction of a watt.

Shelf Labels

Experimentation with the electronic shelf tag systems is wide open. If you own a scanner (see Sam Morse's article in 17:4), bring it along the next time you go shopping and see what you can pick up. Perhaps this communication can be disseminated for a better understanding of the whole process. If you happen to wind up with one of these labels in your possession, take it apart and see what's inside. Or better yet, try feeding your own signal to the label. Those LCD readouts are alphanumeric, so you're not limited to displaying prices. There is still the question of how the label displayed the data even after the battery was removed and replaced. Are those transmitters constantly transmitting price information, or does the tag have a storage capability? If there is storage, what other information can be found on an ESL? If you happen to work for the supermarket and have access to that back office server, well, you've got an entire network of shelf labels to explore. Just remember that changing the price of your favorite frozen pizza to a nickel is not something I recommend.

Supermarkets make only a percent or two profit for each transaction. That such businesses would invest in such elaborate pricing systems poses many questions. For example, how often are prices changed, to what degree, and when? Who is benefiting from electronic shelf labels - customers or the supermarket corporations? If you're a conspiracy theorist like me, then the answers are obvious.

anomaly detection systems, part II



by Thuull

In my last article, "Anomaly Detection Systems" in 17:3, we explored the general concepts behind intrusion detection, a means of classifying intrusion detection systems, and a brief outline of a simple passive/host-based intrusion detection system on a Linux platform.

This article will outline a couple of different ways to accomplish anomaly detection on large heterogeneous networks cheaply and efficiently, from the passive/network-based angle. We'll also discuss signature-based IDS systems' usage in conjunction with anomaly detection to create a well-rounded overall intrusion detection solution.

I can't stress enough the necessity of understanding the traffic flow on your network. If it is your mission to protect that network, how can you protect it if you don't understand what is there? How many web servers do you have? What are their IP addresses? Do they use SSL (443/tcp)? HTTP (80/tcp)? Find out... only in knowing what belongs on your network can you spot what doesn't belong. If you can't spot what doesn't belong, then what doesn't belong is just going to keep on not belonging, without you knowing about it.

I discussed in my last article the fundamental vulnerability that exists in all attack signature-based intrusion detection systems: they cannot "see" zero day exploits. Generally, there is a period of about one week to nine months between the time that a new exploit is created for a recently discovered vulnerability and the time that the attack signature for that vulnerability finds its way into your attack signature-based IDS. So, until you have the signature, what will your IDS system tell you? Absolutely nothing. Won't even see it.

A solution to this fundamental problem? Learn your network, know what belongs, highlight what doesn't. Say your NNTP server has only two ports open: NNTP (119/tcp) and SSH (22/tcp). An attacker doesn't know that those are the only two ports open on it until the attacker probes the machine. If the attacker is smart, he'll hit the machine with one packet a day from a different IP address every day. Will your attack signature-based IDS show a single SYN packet to port 23/tcp? I don't think so. Anyway, back to that solution... collect all traffic that crosses your network at a chokepoint, then bounce that traffic off of a filter set that siphons off all traffic that belongs. What you have left is everything else. You'll find in investigating this "everything else" that about 90 percent of it turns out to be system misconfigurations or what-not on either your end or the other end of the comms stream. However, the remaining 10 percent are malicious. In the above example with the NNTP server, write filters that ignore port 119 and port 22, and have the system show you everything else. You might even want to only filter out incoming traffic to those ports that are from IP addresses that you know should be using those ports. Everything else is suspect.

If you're paying attention, you're probably screaming right now: "What about an exploit against SSH or against NNTP?" Well, two answers to that question. Yes, incoming traffic that is malicious can match a filter that you put in as "normal" traffic, but 99 times out of 100, more than one port is going to be checked on the system before an actual exploit is launched. That, and someone probing for port 119/tcp on your systems will most likely look for it on other systems as well, which should show up in your system because you're not filtering 119/tcp from other machines... only from your NNTP server. The second answer: this is where attack signature-based systems come in. If the exploit used is old enough, your IDS system will probably have a signature for it, and will flag the attack. This covers the hole created when an attacker's traffic matches valid traffic that you would expect to see, to a certain point. This does not provide a solution for when an attacker uses a zero day exploit that matches expected traffic. Still though, you will probably see traces of the activity on other machines.

Do you use firewalls? I bet you probably do, unless you're running a small network at home where you can easily keep up with all the latest vulnerabilities. An effective anomaly detection system can be "built" with the firewall(s) that you're currently using. Leverage your firewalls to be your eyeballs into what's coming in and going out of your network, not just as a simple barrier. Every firewall platform that I am aware of has the capability of not only logging traffic, but of filtering information that is displayed in the log files. Generally, this is used for troubleshooting network issues... did the traffic ever reach the firewall? Run a filter on the logfiles to look for that IP address, if it's not there, it didn't make it to the firewall, etc. But, those filters can be used the other way too... instead of writing a filter to show a specific something, write a set of filters that hide a set of specific somethings... those specific somethings being all traffic that belongs on your network. Filter out all traffic to port 80/tcp on your webservers (and 443/tcp if you're using SSL), port 20/tcp and 21/tcp on your ftp servers, 53/tcp and 53/udp on your DNS servers, etc. Remember, you'll want to be able to see port 53/tcp and 53/udp connects to everything except for your DNS servers, so write your filters specifically for individual machines. Normally, firewall systems will allow you to save filter sets... use them. Check them every day. Log the anomalies in a database, to look for trends later. I once identified a very patient fellow this way, plugging away at the network with two or three packets a day against a different port from a different IP address every day. All put together, they added up to a portscan... amazing. By the way, on that one, RealSecure never saw a thing... of course, you can't blame it; that's not what the IDS systems that are out there today are designed to find.

There are two other ways to accomplish this in passive/network-based mode. You could put Linux machines out in front or behind your firewalls (at prominent chokepoints), or off of monitored switch ports running ipchains in accept all but log mode, run logcheck against your logfiles every hour and have it report anomalies to your email. You could even

write your ipchains rules to do the filtering for you... i.e., accept and don't log 80/tcp to the webservers, but accept and log all else. That would keep log files down some. Or, you could take the Shadow IDS system from the CIDR project and revamp it a little.

The Shadow system is already designed to suck in all the traffic on the network via tcpdump and store it in massive logfiles for after the fact analysis. Filters are then written using normal tcpdump syntax to grep out of those logfiles traffic which matches certain criteria... i.e., you can write a filter to run through and check specifically for individual attacks. However, with a little modification, you can rearrange the system to instead of going in and pulling out the stuff that you want to see (which requires that you know what you're looking for before you look for it), you can have it go out and filter out all of the stuff that you know belongs on the network and report to stdout whatever is left. Hello, anomaly detection.

Let's talk briefly about limitations. Anomaly detection is not the end all answer here. I strongly advise a combination system. The methods that I've outlined do not include things like fragmentation reassembly, MTU size, low TTLs, etc. However, I guarantee that with a combination system, you will see far more than you would with an attack signature-based system alone.

As far as attack signature-based IDS systems go, if you are looking for a system to use in conjunction with this sort of anomaly detection, my suggestion would be the Dragon IDS from Network Security Wizards. I'm personally very impressed not only with this system's ability to find and identify known attack signatures, but its usage of more all encompassing "built-in" broadbased filters that are based upon parameters that catch certain "classes" of attacks which share similarities with known attacks. Essentially, this means that in some cases, new zero day exploits that are modifications of known exploits, or work within similar parameters, will be at least highlighted for further analysis. And that's just the built-in functions... you can write your own rulesets for it that turn Dragon into an anomaly detection system per the style above, simply by having your rulesets ignore everything that you expect to see on the network. Take a look at it, they're doing some neat things.

My point here I guess is simply this: You can't go into intrusion detection expecting that you know what to look for. If your system(s) get compromised via a vulnerability in a service and not by some misconfiguration error that you've made, one of two things has happened. Either you are stupid and didn't patch an announced vulnerability, or someone used a zero day exploit against you. (An academic note here: from statements earlier in this article, you should be able to surmise now that I believe that attack signature-based systems are only useful to stupid people (caveat: That's mostly a joke, there are valid uses for attack signature-based systems for smart people).) If you are smart and have patched everything that needs patching, you're still not secure, but you can at least see the attack coming from the other smart guy sitting out there somewhere. And if you're really smart, then your systems are probably tight enough that it's going to take that other smart person longer than he wanted to in order to compromise your network. This gives you the opportunity to do something about it before anything ugly happens. Let's face it, it's like a big game of chess... sometimes the other guy is smarter than you are, and you get to learn something.

Strange Love

Or, How I Learned to Stop Worrying and Love the Anna Kournikova Virus

by 6M AL

It's odd the people you keep in your address book. As a reader of *2600* for the past eight years, you learn a lot about what people will and won't find offensive. You learn that people will complain about things that affect them, and won't complain if it hasn't affected them yet.

When I received the Anna Virus, I knew it for what it was: a program created by some hacker that had been sent to me unwittingly by another individual. I guessed it might be a worm that would be sent out to another user after an inadvertent reading or clicking of the e-mail message containing it.

I clicked.

Within minutes I was receiving phone calls and e-mails, some laughing and joking, others solemn and angry, from all the people in my address book. Some were asking what I had sent, one man even wanted help opening the attachment. "I'm sure she's hot," he replied. "But my mail program won't open the picture."

I had sent e-mail to people who owed me money, to people I am in litigation with, to women I haven't called after an affair went sour, to men I had admired, to persons I had feared.

Worst of all, I hadn't just sent an e-mail. I had sent them the virus.

It took a few hours to sink in - the potential impact of what had happened - and you can imagine that I could have been angry. I could have been dismayed. But I had made the choice to try the virus anyway. I had been in good company. CNN carried news of the virus well into the next few days. I was elated and disgusted at the same time. I had burned bridges and made others laugh at my actions. I felt happy I had made no mistake. I had run the virus on purpose.

Now the most important question many would ask is why create such an ugly virus? "Why do hackers have to waste so much time and money on destructive forces?" they demand to know. My response is simple. If the virus I received had short-circuited my copy of Windows, if it had sent instructions to my hard drive to reach for a sector that didn't exist, gouging a new hole in my storage space, the Anna Virus would have been wrong and sickly twisted, something I could hate.

But it didn't. It taught me, and many of you, a lesson. It taught us to guard against such threats and to be ever wary of what we see and open. It took nothing from me, nothing but a little pride, which I could make do without. And the Anna Virus introduced me to people I haven't spoken to in a long, long, time.

Their e-mails may begin with "I think you have a virus...." But they all end with "So how are you doing these days? How is life?" at the end.

DECLAWING YOUR :CUECAT

by Lunius

Cuecats are barcode scanners given away with issues of *Forbes Magazine* and at Radio Shack. The Cuecat is used to scan a bar code of anything you find interesting and the CRQ software, included with the cat, uses the default browser to bring the user directly to a corresponding web site with information from a database. What they *don't* tell you is that every time you do this, a serial number is sent to them telling them who you are (remember giving your name to the Radio Shack guy?). And while it is possible to change this, they try pulling technicalities, saying that the cat isn't even yours - that it's only on lease. They say this so that you cannot legally open it and reverse engineer it! Too bad nobody gives a fuck. Intellectual property laws protect reverse engineering for competition last I heard, although corporations have been disagreeing lately.

Operation and Reverse Engineering

The Cuecat is a keyboard wedge scanner like several other bar code scanners, meaning it plugs into the keyboard slot on your computer, and the keyboard plugs into it. When you scan a bar code, a line of information is sent like the following:

.C3nZC3nZC3nZCxj2Dhz1C3nX.fHmc.Dx-PYE3b6C3nZC3jY.

This is four pieces of information separated by dots.

1. ALT-F10 is sent as a wakeup signal.
2. The serial number of the wand is sent.
3. The type of bar code (UPCA, ISBN, etc).
4. The actual barcode information.

Now, as you probably can notice, the information is encrypted. Jean-Phillipe Sugarbroad is credited with figuring out that the Cuecat uses a modified version of base 64 encoding, a very simple form of encryption. Take each block of four characters and convert them into six bit values by indexing into "[a-z][A-Z][0-9]+-". String the four six bit fields together to get a 24 bit value containing three bytes. Exclusive OR each with 67 and you have three decoded bytes. Strings that aren't a multiple of three characters are zero filled and they should be stripped out if it isn't being processed by C code which takes a NULL as the end of string. According to the driver from Lineo, some cats don't encode the same. For these you index into "[a-z][A-Z][0-9]./".

You can do this yourself, or as any sane human would, with a script. You can find a small perl script which I like best, nicknamed the "tatooable version" for its short, short length at http://opensource.lineo.com/cuecat/.

Decoded, the aforesaid line is this:

0000000000215756002 UPA 691839000011

"UPA" stands for UPC A and the "691839000011" is the bar code number. The part you must worry about is the first number: the serial number. Getting rid of the serial number is relatively easy. All I had to do was cut the Data Out circuit on the Hyundai chip and the Cuecat now sends garbage for the serial number. (The chip will either be an eight pin device or a smaller five pin device. Be sure to cut completely through the trace.) More information on this can be found at http://www.ma2600.org/-index.php?page=declaw.

Congratulations, you now have a Cuecat that doesn't send a serial number *and* you know how to decode the barcode number. To take advantage of this you can find software at lineo.com or at ma2600.org to take inventory of your book/CD collection, or even to create your own bar codes. Have fun.

Shout outs to Ohmboy, Christ, Rasputin, Morn_Star, MA2600, and countless others who have guided me.

UTP
Digital Directories

INTERNET BUSINESS GUIDE

2600 Magazine
P.O. Box 752
Middle Island NY 11953
USA

DATE 22.Dec.00
REF. NO. IBG/7211318
ENTRY PERIOD -> DEC 2001
AMOUNT US$ 960,00

ENTRYOFFER - COMPANY ENTRY

The specified data will be published in the Internet Business Guide when payment has been received. If the publishing house is not notified of any amendment wishes or supplements, the publication will appear in the following directory:

Internet Business Guide / Country : USA
SICode : 2721Periodicals: Publishing, or Publishing and Pri

Item	Subject of the cost estimate	Currency / amount
001	Online Publishing for specification above and contact numbers listed below. Com# Fax : 516-474-2677 Phone : 516-751-2600	US$ 960,00
	total	US$ 960,00

The data printed out above will be published as specified. If any amendments are necessary, these may be communicated online in the Internet. If you communicate any amendments by mail or fax, please give us your reference number and specify "Amendment" as the reason for your letter. You can find the sector headings at the UTP web site. These may also be requested in writing in the form of excerpts.

In order to guarantee processing in due time, please pay the indicated amount within 10 days of receiving the offer. In the case of remittance to our specified account, indicate your reference number as the reason for payment. In the case of payment by cheque, please also specify your reference number.

Terms of business overleaf

UTP AG
P.O. Box
CH-8583 Sulgen
Switzerland
Fax: +41 (71) 6 400 500
E-Mail: info@utp-online.com
Internet: www.utp-online.com

Banking connections:
Postfinance
CH-9000 St. Gallen
Account: 87-32112-9

Raiffeisenbank
CH-8583 Sulgen
Account: 81411-23395.85
Swift Code: RAIF CH 22

LOOKING FOR SCUM? No need to look further. These people go around sending these "entry offers" to companies for some ridiculous online "business guide." Doesn't it look an awful lot like an invoice? We suspect hundreds, if not thousands, of unsuspecting businesses just pay these things because they look like bills. UTP, along with another Swiss company called IT&T (www.ittag.com) have been sending these little swindle applications to the listed address for every Internet domain we registered through Network Solutions Inc. Incidentally, neither one of their web pages even worked when we tried to access these alleged business guides! But they have that covered too - both companies have almost identical statements on the reverse claiming that they are not liable for delays as long as they're not the ones responsible for the delay. Slick. Refunds are simply not given under any circumstances and once you register with these crooks, they will automatically bill you year after year until you send them a registered letter telling them to stop. As a public service, we're going to add these two companies to our own "business guide" - and we'll do it for free!

Letters continued from page 39

Voting Ideas

Dear *2600*:

I was appalled at the methods used for voting. This was my first year voting for the next President and like a good happy citizen I shuffled my way to the elementary school in my area and put in my vote... on a plain sheet of paper by marking in a circle with a "specially designated pen." Upon further examination the pen appeared to be a Sharpie marker. Kind of outdated, isn't it?

Of course, many are in search of another way to make the whole voting procedure work. Using a web site or online database would be a problem because of Internet security. But there are other alternatives! I am the Oracle Database Administrator for an Internet company in my state, and can see where a good database application could come in handy here.

First, each voting area would be equipped with computers networked together. There would be one central computer for each center running the actual database, and several client machines running the actual forms used to input data. A voter would walk in, click some radio buttons (or drop down lists, etc.), and walk out. When voting was closed, all data would be in this main server, and a preprogrammed report could easily print out, e-mail, or just save all statistics. It would also produce an encrypted dump file of all voting data, which would be sent to (by means of a burned CD, a ZIP disk, or ftp) and imported into the main database for the state once voting was finished to count up state votes. Or the dump could be loaded as a separate database on the main state server, and replication could be used to pass over the necessary data. Again, a report can produce statistics.

Because of the contracts the government has with Oracle, I cannot see a system like this costing very much in the way of licenses. The computers would probably be the most expensive part, but the clients wouldn't have to be state-of-the-art machines by a long shot!

SiON42

Dear *2600*:

I just finished reading your comments to chrisbid about the voting fiasco in Florida. You said anything is potentially better than the current system, so here are my thoughts.

I thought of using USB devices for the input and using a USB hub to connect multiple devices to one computer. Where I live we use the infamous punch card system, where when you flip the page it exposes another row of holes for you to punch. So I thought I could keep the idea simple and have a similar setup (I wouldn't want to get people confused again). Instead of voters inserting and removing cards the area under the matrix of holes would be replaced with the USB devices. The USB device would have a switch and an LED for each hole in the current machine. When you insert the poker tool it presses a small switch, which lights an LED inside the hole. Selecting another candidate for the same office would remove the previous vote and turn the light off (through a hardware XOR). You would have to add two more steps though, actions to start and stop someone's voting period. Easy enough - when the poker tool is removed from its cradle the session is started and when it is replaced the session is ended, period. Now, you criminally inclined are thinking something which I am getting to. In order for the machine to be able to start a session, the poll worker has to activate the booth. They will do this once you hand them your ID. (Here they take and check our IDs and our voter registration card to make sure we only vote once. Maybe, I could also add a bar code scanner to scan IDs in quickly.) Once a session is ended, the voting machine has to be reactivated by the poll worker before a new session may begin. I may want to add a step that doesn't allow the session end to commit the new data until a new session is started or the poll is closed. This would allow poll workers to clear the session if some less intelligent voter made a mistake and ended their session early.
I am not a USB expert, but I believe that each device connected to a computer has to have a unique identifier. I have never connected two of the same peripheral to one computer via USB, so I am really not sure how this would work. But, if they did have to be unique we could have a series of color or letter coded devices, so that a poll worker wouldn't connect two devices that would cause a conflict.

Now more on the poll worker end of the plan. I start by connecting those USB hubs to Windows machines. We would use Windows machines for a variety of reasons: One, Windows offers good USB support. Two, *NIX machines would require an operator with some intelligence. Three, I don't care for Macintosh toys. Four, and most importantly, most governments already have Windows computers. See, I am slightly Libertarian and I hate when government spends more of my hard earned money. Also, every time I have voted, it has been in a school and I know (around here at least) they have Windows computers in the schools. And, since we are talking about money, the USB devices should be manufacturable for a fairly low price. There are tons of kids' toys selling for a couple bucks that are technologically more advanced than my proposed devices.

Now to the software. I would provide each voting computer with a single CD, off of which the voting device drivers would be loaded and the voting software would be run. The software would run a database to store the votes and provide an easy GUI for the poll workers to use. Each voting computer would also get a series of 3.5" disks, to which the votes would be recorded. The votes may reside on the hard drive during the voting process, but will be automatically transferred to disk when the polls are closed. The 3.5" disks would be taken, via courier, to the elections board, just as they are done now. This leaves out networking for now, because I don't feel we are ready for that. A temporary government network is a disaster waiting to happen. It's temporary, it's government, it's a computer network, it ain't happening in the near future I'm afraid. The good thing about my method is that it could be easily upgraded to have network support in the future just by upgrading the software. Then again, you could have the program dial out via modem to the Board of Elections once the polls close. These are my ideas. I just hope someone some day will actually improve the current system.

cstoll

Reusing existing computers from a school probably isn't such a good idea considering the many weird pieces of software that could have been installed during their stay. And it's possible someone could come along with a bunch of identically marked floppies and steal the election. There are some good ideas here but we invite our readers to try and tear this and other proposals apart as it's the only way we're going to get anywhere.

Dear *2600*:

Don't mean to brag too much, but in late November while everyone was still trying to figure out if Gush or Bore had won the election, Canada had an election too. A country of about thirty million people across six time zones (and the second largest country in the world) had all of the votes tallied, by hand, in about five hours. Oh, and the ballot was the same from Toronto, Ontario to Alert, Nunavut. There was a candidate's name and beside the name a big round circle. You put an X in the circle and you had just voted for the candidate. Could it be any simpler?

Michael

Dear *2600*:

Here's the $300 voting machine: a cheap diskless 486 that boots from a CD that holds the info for that precinct and that runs a touch-screen. The voter touches the face of his chosen candidate, the machine asks if he's sure a few times, and at the end the voter is shown *all* of his choices. The machine then burns this to a CD after each vote. The info is also held in nvram for redundancy. The machine is locked in a box with no keyboard, just the monitor. Only the monitor needs to be in the booth. At the end of the election the machines are impounded (to preserve the integrity of the nvram) and the WORM CD (not rewriteable) is collected and tallied. This system can't be screwed with and is nearly idiot proof (except for the mandatory idiot candidates that we can't seem to get rid of).

anon

Article Feedback

Dear *2600*:

Regarding "Microsoft's Hook and Sinker," LeXer was close but no cigar. The revenue stream from all the certification programs is insignificant relative to the other business Microsoft does. Most of the revenue is generated and retained by the businesses running the system including the test administrators, the educational facilities, book authors, book publishers, and the rest. Also, the information to pass the exams is not solely learned by attending their courses. Web sites such as www.braindump.com and test preparation services such as Transcender provide the necessary information. Further, it is impossible to expect to learn how to administer an operating system as complex and quirky as NT 4.0 or Win2K effectively without working in the environment, discussing matters with other admins, and keeping abreast of the current release information. That is the true way to pick up the "tricks" and inside information that lead to proficiency. The main reason is that the NT 4.0 exam is based upon the original release of the operating system from 1996. The software is constantly evolving and the exams do not take that into account for other reasons.

Only in the last paragraph of your article did you touch on the correct reason for Microsoft's trickery. Microsoft sought to set the certification standard artificially high to increase the value of certification to both the certified and the operating system through the perception of standardization regarding their unstable products. Rather than create a stable and efficient product, Microsoft tried to develop customer confidence by instituting a professional certification system that created the appearance of stability and high standards in a profession sorely lacking critical measures for employee skill sets. Once again Bill Gates proved a better businessman than a software developer. Experience is the real teacher but one needs an MCSE degree to land one of the better jobs. The employer's perception is manifold. When the hiring process begins, it is easier to separate the men from the boys, or so the employer thinks, by requiring a certification. He can more easily justify the hire of an admin at a higher salary based upon paper credentials. Lastly, the certified can demand a greater salary based upon their credentials.

Ironically, the reality could hardly be farther from the truth. I am not certified yet I am responsible for administration of my organization's domain. The other professional IT staffer and I have three people working for us in our IT department. We have worked through many a "paper" MCSE - people able to pass the tests yet unable to handle the work.

Sorry LeXer, maybe when you have worked in the field for a while you will have a better understanding of the situation. By the way, there are many exceptionally good reasons to loathe Microsoft; you got that right!

reuven

Dear *2600*:

Ok, to start, I love you guys to death. You're my heroes... mostly. Great job on 17:4. Lotsa neat stuff.

Now, to the point: page 44 of 17:4, "Radio Shack's Newest Giveaway." Sorry, guys, but you totally blew it on this one. This had to have been sent to you from some tweak at Digital Convergence to get more coverage on this gizmo from hell. The major point here is that unmodified, this thing transmits a serial number back to DC, which links across to the registration info you gave them on yourself when you installed the software to interface it. Getting this? You're plugging a product that gives Radio Shack and Digital Convergence *loads* of demographic info, right down to your e-mail address or telephone number (whichever you think is more important), each time you nail a barcode with this thing.

The article totally missed the point of the modability of these things - that the serial number's kept on a chip onboard the godawful little thing, that can be disabled by cutting ground on the chip; and that by running a lead from the positive voltage onboard the thing to one of five test probes on the board (position varies from one board rev to another), the thing can be forced to output straight data, non-uuencoded.

Give this a shot - open up a text editor and scan, straight into it, with one of these things. Three fields: 1 is the serial number, 2 is the barcode type, and 3 is the barcode data, all uuencoded. The device this kid is brag-

ging about is cursed, and ain't useful unless people know the story on it, and what it's being "given away" for. All the rest of the data on these things, right down to a BOM for each revision, is available with a couple of searches.

Sorry for the rant; just had to get that out of my system.

Tim

And you were right to do so. While the points you mention were widely known when we printed the article, there was no way we could add them without writing an entirely new article, which we just didn't have the time to do. But by running the existing text, we got no less than nine new articles with additional info, one of which we have printed in this issue. We hope people remember that this is the way 2600 works - our info may not always be 100 percent but with some fine tuning and reader input, we can keep getting closer.

Dear *2600:*

"New radios would have to be bought" [if community FM takes over current VHF TV frequencies]? *Not.* My Sony Walkman (and lots of other units *now* out there) have a Japan mode that receives broadcast FM down to 76 MHz. Just give us TV 5 and 6, Fox Charlie^2. We're already prepared.

v-dick

That makes it an even easier transition. But the only way this is going to happen is if the proposal becomes known throughout the nation - namely, allocating the future vacant audio signals from analog TV stations to community radio. It's vital that these new stations not be commercial or part of any existing broadcast network.

Fun in the Stores

Dear *2600:*

I just yesterday picked up the new issue, 17:4, and was chuckling at the cover art while paying for it when one of the store clerks said to the one who was serving me, "Did you get any ID for that?" The one helping me out said, "No, I thought I'd let it slide this time." I naturally asked what the hell he was talking about, and he told me that they normally have to take three pieces of photo ID from anyone buying *2600*, and once a month the list is forwarded to the RCMP (Royal Canadian Mounted Police) and CSIS (Canadian Secret Intelligence Service) who then forward the list to the FBI. I was taken aback for a moment, thinking that Canada had finally gone to hell, when the two clerks started laughing their heads off and one gleefully exclaimed "Gotcha!" Boy, was I relieved.

The fact that I had to take that possibility seriously serves as a testament to the ever-growing tensions regarding freedom of speech. As I understand it, one of the fundamental freedoms guaranteed under the Canadian Charter of Rights and Freedoms guarantees "freedom of association," inherently covering literature. I've read horror stories about bookstores keeping *2600* behind the counter and only available upon request, but requiring ID would have made me want to go home and hide under the bed. I would stress to everyone in Canada and any foreign nation to keep in mind that just because things like the DMCA pop up in the US doesn't mean that the rest of the world is asleep. We've got to be just as aware of threats to fundamental freedoms that are going on within our own borders as well as internationally. Luckily, what I encountered was a joke, but it could happen.

In the meantime, I'd like to congratulate the guys at Toronto Computer Books for scaring the pants off of me. Good work.

xcham

Dear *2600:*

So the other day I was at Babbages just checking out stuff when I overheard some other customer say to the clerk, "Hey, do you guys sell tone dialers?" Instantly I looked up to see a group of three junior high aged kids, a confused looking clerk, and another customer shaking their head in disgust. The clerk said, "Ummmm, let me go ask my manager." Just thought I'd share another story on how stupid people really are. Come on, of all the places to go and ask for a tone dialer, why Babbages?

AquaGlow

We're wondering how the other customer knew to be disgusted. But let's not program ourselves to think this way. There is nothing wrong with buying hardware and even if you're 99 percent sure how these people intend to use it, you still don't know for sure.

Legal Questions

Dear *2600:*

If someone were to, say, memorize the entire DeCSS source and could repeat it perfectly so that someone else could write it down, what would the MPAA do? Sue the guy (or gal) for his memory? Or just tell him not to tell anyone? And what would happen if someone got it tattooed on themselves, someplace obvious, then walked around on the street showing it off? What exactly could the MPAA do? Is a tattoo, in fact, not a work of art?

Joseph

Dear *2600:*

I am from Canada and was wondering if any countries other than the US have laws similar to the Digital Millennium Copyright Act?

Hy Stress

Unfortunately, with global bodies like WIPO, the WTO, and more regionalized entities like NAFTA and the European Union, it's become far easier to get such laws passed throughout the world. A cousin of the DMCA known as the Digital Agenda Act recently came into existence in Australia, technically making it a crime to forward e-mail without permission. We fear there will be more ill-conceived legislation worldwide before this is over.

Advice

Dear *2600:*

I am an administrator at a school, and I wanted to give the readers of your magazine the perspective of an administrator regarding student IDs, computer networks, hacking, and education in general.

People do not go into education for the money - there isn't any. They go into education with a desire to teach students to think. All your teachers, administrators, and counselors all got into education to make a difference. Today they are dealing with a small percentage of very troubled kids who have been abused at home, are neglected, regularly use very addictive substances like coke and heroin, engage in violence and prostitution, and threaten violence on a daily or monthly basis. It is hard to create a nation of literate free thinkers when you find out that a kid is talking about suicide, his/her parents don't provide enough food, the 12 year old is sleeping with both her father, uncle, and aunt at the same time. Your teachers may be a bit distracted over these issues. I just wanted to teach Plato, Malcolm X, and Gandhi. Now I have to deal with a society in crisis and parents who just don't care about their kids, and some teachers who are not up for the job.

Every event creates a reaction and the reaction to this crisis has been the creation of factory schools (2000+ students) and large classes (35+). As your readers know, it is impossible for kids to get the kind of true education where you learn to think for yourself, solve complex problems, and develop a system of ethics based on responsibility to your community and the world in this kind of environment. Schools are teaching students that they are numbers, as the letters of JoePUNK102 and data refill attest. I do not think that this is part of an organized plot to eliminate freedom and liberty. I have worked at several public and private schools. Sorry, the average teacher and administrator are not that smart. They are just trying to maintain some measure of control. Ninety percent of the students who I have encountered are not a threat to themselves or others. However, there are a lot of troubled kids out there. Run the numbers. If your school has 2000 kids, 200 of them will be involved in some major crisis at any given moment. This takes up a lot of time, and prevents me from teaching you Plato, Malcolm X, and Gandhi.

If you don't like your ID cards, organize a strike and burn the cards in a public ceremony off school grounds and after school hours. Get the proper permits from the police and fire departments, call the TV stations, and get the press involved. An act of rebellion means nothing unless it get some press. Study Gandhi and use him as a guide for your acts of nonviolence and civil disobedience. Get the students of your school to wear coats and ties and march in mass to the town square. With permits in hand and news crews watching, set fire to the permits. Make sure that nobody is going to get hurt. A person has to agree to be oppressed.

Computer administration is the bane of my existence. Any smart administrator knows that the kids are more sophisticated than any adult when it comes to running a network. Most public schools do their IT in house. Usually the technology director is a burned out teacher or librarian who is near retirement. That is all they can get. The old geezer is scared out of their wits by the 13 year old who knows more about network administration than he/she does. They have no control and that drives them crazy. You can make a lot more money in the private sector so you are always dealing with somebody who is way over his or her head. You have three options as a student:

1. Hack the network and make it your own. Realize that your teachers know more than you think. I cannot believe what students leave lying around on their open accounts. If you hack a system, you will make mistakes and sometimes these will bring the system crashing down. Then your old geezer technology director will be brought into the principal's office and somebody will pay.

2. Get your school to give you old equipment or set up an organization that accepts computers from businesses and corporations in your area. Download UNIX and create a student network of your own. Most principals will go for this idea if you get a member of the student government to sign on to it. Tell them that this will cut down on the problems that the school is having with their own networks, and that this will help you get into a good college. (Administrators and teachers love this sort of thing.) Get started on your Beowulf cluster.

3. Do nothing and remain a pissed off alienated teenager, hacking into a bullshit school system.

It is sad that I have to tell you the following truth. If you are from the middle-class, and are an average student, you are getting a very poor education. You need to educate yourself. Start off by getting a group together and picking up the *Autobiography of Malcolm X*. Read the entire book and talk about it with your friends. It is the story of a man who educated himself. If you are living in the burbs and are white, it is especially important for you to read this book, but be aware that this is a very subversive act. Then read the Plato's *Republic* and get ahold of a really good book on UNIX. A philosopher/hacker will have a bigger impact on society than just some kid smoking dope, watching TV, and wasting his/her time. A hacker is a revolutionary, and there is no more revolutionary or subversive act than to become educated.

I wish I could have a school filled with hackers. I'm waiting....

noname

Technological Nightmares

Dear *2600:*

In response to the comment by data refill in 17:4 and the editor's comment, there is a technology that allows tracking of your toddler. The child wears an anklet, similar to house arrest anklets, and the parent/guardian/hacker who has access to a custom web page can track the exact location of the child through Global Positioning System from anywhere in the world. Personally, I think this is a retarded thing to do. But that's just me.

Xerxes2695

It's important to explain why though. People will take your position more seriously.

Dear *2600:*

Back in mid-November, I decided to get DSL service. I was told it was available in my area. I was told it would take two weeks. That was almost three months ago. The turn-on date has gone from December 5th to December 18th, to numerous other dates, to "pending." I give up.

Jeffrey

You think you have problems? It's standard practice where we are for Verizon to claim that a location doesn't qualify for DSL when the order is placed through a competing ISP. But they will then offer to hook the customer up if they agree to use Verizon as their provider. This has become so commonplace that ISPs actually tell customers to expect it.

Dear *2600*:

I thought some people out there might like to know about a new thing taxi companies are using for their dispatch instead of the radio. It's the new MailStations. They're really cheap ($79) and it's a good idea for the companies to use because with the e-mail there will be no messed up address since it's right on the screen. The e-mail for them works like this: If the company is Yellowcab, it would be carnumber@yellowcab.com. Just play around with it until you get it to work.

^CircuiT^

You've inadvertently explained why this is a BAD idea.

Dear *2600*:

It appears that each and every individual entering the stadium for the Super Bowl had their "face scanned." I'm happy and grateful that law enforcement is looking out for all of us in this sweet Orwellian fashion. Aren't you?

Dalai

And the only reason we even know about this is because they chose to tell us.

Dear *2600*:

I've been a reader for all of two issues but I like what I've seen. I was just wondering if any of the *2600* team or the readers had seen the piece about the software used to identify terrorists at the Super Bowl. Apparently it was never, ever designed to be used with a large crowd. In the report, they showed just six people walking past a security camera. One of their images had been specified as a known terrorist (no, he wasn't really) but the software failed to identify him because it didn't have time to collect multiple images while other people were walking around. In fact, the results often merged two or more faces together, creating images of nonexistent people.

Wow. Not only do they invade your privacy, they do it badly.

The_Chaotic_I

Don't worry, they'll get better.

Offerings

Dear *2600*:

First off, I myself am not a hacker. I try to learn everything I can about the subject but I don't have the mind to sit still for eight hours trying numbers. Recently I got a job working for a survey firm that dials nationwide going over the phone surveys for such companies as NASDAQ, Prudential, Fidelity Investments, and such. In doing my eight hour shifts of dialing and dialing, I frequently come across data lines. For reasons which I can't explain (even to myself), I began recording these numbers. I have over a hundred now and I get about ten a day. Many of these numbers are probably just harmless business numbers but since our dialing is completely random, I'm sure there is something interesting in there. I am wondering if *2600* would be interested in these numbers for personal use or for print. They are yours if you'd like, and I can get you another 20 a week if you want them updated. Let me know.

Simon Jester

It used to be that lists of interesting and mysterious numbers would always be circulating in the hacker world. There are certainly more numbers now than ever so we would welcome any such list. If all the telemarketers did this for us, we might cancel some of the contracts we have out on them.

From The Inside

Dear *2600*:

First, I must let you know how much I enjoy your zine. It kicks ass - straight truth, facts, and pure knowledge without any mind polluting commercial advertising crap. Sadly, now even *Mad Magazine*, a favorite of my youth, has caved in to korporate kash and begun to accept advertising. How sad!

Most importantly, I have to give props to my friend Zyklon for reintroducing me to *2600*. I hadn't read one since the early 90's. I'm also very pleased to say that at 8:00 am PST today, Zyklon went home. Released from this freaking hellhole. Unfortunately, like Kevin, he is not free for a few more years. He said that if he is lucky, his P.O. will be mellow and let him use a computer. It is under very unfortunate circumstances that I had the opportunity to meet and get to know Eric a little. But I certainly am quite glad to have met him and am pleased to count him among those few I call friends. He is an individual of great intelligence. He was, like others, seriously misunderstood and feared for his knowledge.

James

Dear *2600*:

Hi! With only seven or so hours of incarceration left, I thought I'd write and thank you for all you have done for me, and for spreading information to the public to help fight the good fight. It was a good experience seeing our country, our society, and our government in action, and I have come to see what *2600* really stands for.

I wish you luck with all your troubles, current and future, and hope for all our sakes that reason and freedom will prevail.

Eric Burns

Welcome back. Putting someone in prison for simply hacking a web page still seems unbelievable to us. But we're glad you're out and keeping a positive outlook on the whole thing. Further proof of a non-criminal mind.

"Takedown" Taken Down

by Emmanuel Goldstein

As a race, we must always redefine our boundaries. That which was impossible in the past becomes attainable and even commonplace in the future. The boundaries of tolerance have been in constant movement since the beginning of recorded history. Indeed, even the boundaries of space itself - the very edge of the universe - have not remained constant.

Takedown is a movie that redraws the boundary of bad. To critics and movie buffs, this will be an inconvenience, as long established champions of bad cinema such as *Plan 9 From Outer Space* or *Waterworld* may lose their spot in history to this relative newcomer.

At *2600*, we had to go to a bit of trouble to actually see this film. Since it's already been released in various countries around the world, it's now possible to see a video or DVD copy if you order it from one of these places. (It's still a no-show in the United States and after finally seeing it I can understand why.) We got ours from France - via www.amazon.fr - where the film goes by the name of *Cybertraque*. Note that you will need a DVD player that can get around the region-locking nonsense that makes it a pain in the ass to view foreign movies. The irony here is that this is an *American* film which most Americans are technically unable to view. Not that very many would want to, but the choice should be theirs.

You see, none of us wanted it to come to this. We tried to stop this grossly inaccurate and unfair portrayal of the Kevin Mitnick story as soon as we found out about it back in 1998. It was based on an equally distorted and biased book of the same name written by John Markoff and Tsutomu Shimomura way back in 1995, the year Mitnick was arrested. And when we saw the script, we knew something had to be done. I mean, they portrayed this guy as a violent racist criminal who went through life cheating and stealing. The one infamous scene we objected to had Mitnick ambushing Shimomura in a dark alleyway in Seattle where he then clubbed him on the head with a garbage can lid. (That scene was later removed.)

We tried everything to reach the folks at Miramax - phone calls, visits, even a demonstration outside their New York offices. We never got a response. Even when we visited the set in North Carolina, they

wound up literally running away from us. They never believed that all we wanted to do was ensure that the story be told accurately since the guy they were portraying was stuck in prison unable to defend himself. They probably believed that everyone in the hacker community exists simply to create mayhem. Reports that filtered down to us confirmed a high level of paranoia on the set.

So it's little wonder that the film sucks, that foreign audiences worldwide have united in their rejection of it, and that it may *never* get released in this country. Bad storytelling has a way of not working out.

The DVD we received also contained a real life Kevin Mitnick interview, something that surprised Mitnick quite a bit since he had never given permission for it to be included! The attaching of the real-life Mitnick's image to this product falsely implies that he endorsed its release. He most certainly did not.

From the opening moments, *Takedown* misses the boat on hackers in general and Mitnick in particular. TV images reveal the threat and fear of hackers, who engage in widespread information distribution known as "hacker communism." It gets worse. When Kevin and his friend Alex go to meet sleazy hacker "Icebreaker" (based on real-life hacker Agent Steal), it's in a strip bar. "You set up this meeting," Kevin (played by Skeet Ulrich) says disparagingly to the soon to be revealed federal informant. As if hackers operate by setting up meetings in the style of underworld crime figures.

"This is where you get into trouble," Alex (played by Donal Logue) warns Kevin when he tries to find out more information about some computer system somewhere. But Kevin is right there with an even blander response: "I just have to know." Said with all the passion of a manatee.

Passion is just one of the qualities lacking in *Takedown*, where you're left with the overriding question: Why should I care what happens to *any* of these people? There are only two characters I liked in the film and both of them were minor roles - the two techies from Cellular One. Maybe they just seemed like the only human beings in a film of stick figures. I don't think I've ever seen a larger assortment of sulky, sullen, spoiled brats in a single production.

When Alex goes to meet Kevin in a dark alley while he's eluding the feds, he utters what is likely the most prophetic line of this 90 minute ordeal: "Aren't you taking this cloak and dagger shit a little far?" I changed my mind - I like Alex too. Because I know deep down he was aiming that line at the director.

Takedown never seems to synch into an actual plot - at first it's about Kevin's attempts to learn about a phone service that allows any phone to be listened in on. Then it's about a fictitious phone company called Nokitel and the obtaining/cracking of their source code. Then it's Kevin vs. Tsutomu for no particular reason other than Tomu calling him "lame." The ultimate insult. Then it's Kevin running from the FBI and becoming the Bionic Hacker as he leaps over fences in slow motion. And, naturally, in the end it's about a virus called Contempt that apparently can do everything from crashing planes to stealing money. Kevin has to enlist the help of 10,000 university computers to "crack the code" because he just "has to know." All the while the FBI is stumbling over themselves to track him down while Tsutomu sneers in the background at their incompetence.

Apart from the amazing ability to make his face appear on the screens of computers that he's hacking, *Takedown's* Mitnick has no special skills. He's just a nasty person who treats women like crap - he refers to his own mother as a bitch and tries to seduce a big-toothed potential girlfriend into the world of scanning when all she wanted was sex. These little character traits of his were completely fabricated. They only show how the writers didn't care at all about the real Mitnick whose integrity they were destroying.

And don't get me started on the technical stupidity. Who the hell had flat screen monitors in 1994? And why does Mitnick seem surprised that a payphone call costs 35 cents? (He quickly solves *that* problem by holding up a tone dialer to the phone and... *dialing touch tones!* How could anyone dare to call him lame?) I don't know *what* they were trying to imply when an FBI agent was reading a headline and it literally took ten seconds for it to scroll by! And why in God's name does Shimomura refer to an overheard phone call of Mitnick's as a modem call when it's quite obviously to a *fax machine?!*

But the biggest gaffe of all lies in something that was apparently edited out. All throughout the film, the main FBI guy (aptly named Gibson) is walking around with a huge unlit cigar in his mouth - even when he's standing in his house after Mitnick turns off his water, gas, and electric from a payphone. It never seems to leave his mouth. Yeah, it's gross and disgusting, but what the hell is the point? Well, in the script, we realize that this guy only lights the cigar after he captures the criminal. So guess what scene these geniuses decided to cut? This seems to have been patched together with all the care of the people who fill potholes in New York.

But don't take my word for it. Read the profundities of *Takedown* in its own words from various scenes:

"Privacy? Never heard of it."

"This is like no kind of code I've seen before."

"I'm a hacker. Mitnick's a cracker. Big difference."

"When you thought you were talking to Netcom, you were talking to me.
You were the machine?
Yes, I was."

"You did not get this from me. I do not want Kevin Mitnick coming after me."

"He said I was lame!
Kevin, he didn't know it was you."

"The question is how. The question is always how."

In my opinion, the question is *why*. This travesty could have been prevented if only a dialogue had been established. Instead we have a film that actually makes region coding seem like a good idea.